

Specificații tehnice

Numărul procedurii de achiziție nr. ocds-b3wdp1-MD-1723618903452 din 14 august 2024

Obiectul achiziției: Servicii de analiză, consultanță continuă și evaluare a securității cibernetice a sistemelor IT (servicii de scanări de vulnerabilități, consultanță, testare a securității cibernetice din cadrul CNAS anul 2024)

Denumirea serviciilor	Denumirea modelului serviciului	Țara de origine	Produ-cătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
Servicii de analiză, consultanță continuă și evaluare a securității cibernetice a sistemelor IT (servicii de scanări de vulnerabilități, consultanță, testare a securității cibernetice din cadrul CNAS)						
Servicii de analiză, consultanță continuă și evaluare a securității cibernetice a sistemelor IT (servicii de scanări de vulnerabilități, consultanță, testare a securității cibernetice din cadrul CNAS anul 2024, la solicitarea Beneficiarului	Servicii de analiză, consultanță continuă și evaluare a securității cibernetice a sistemelor IT (servicii de scanări de vulnerabilități consultanță, testare a securității cibernetice din cadrul CNAS anul 2024)	R.Moldova	Logical Point	<p>Cerințe pentru servicii de analiză, consultanță continuă și evaluare a securității cibernetice a sistemelor IT (servicii de scanări de vulnerabilități, consultanță, testare a securității cibernetice din cadrul CNAS).</p> <p>I. CERINȚE FAȚĂ DE OFERTA TEHNICĂ ȘI FINANCIARĂ</p> <p>1.1. Prevederi generale</p> <p>1.1.1. Acest capitol descrie cerințele referitoare la formatul și structura ofertei.</p> <p>1.1.2. Este necesar ca Ofertantul să facă cunoștința cu toate instrucțiunile, formularele, condițiile incluse în prezentul document.</p> <p>1.1.3. Ofertele trebuie să fie complete și suficient de detaliate, astfel încât să îi ofere Beneficiarului posibilitatea de a înțelege cu ușurință toate aspectele. Ofertele vor include sesiunile descrise mai jos, fiind întocmite în conformitate cu cerințele față de oferta tehnică.</p> <p>1.2. Oferta tehnică.</p> <p>Oferta tehnică va cuprinde următoarele elemente, dar fără a se limita la acestea:</p> <p>a. Înțelegerea obiectivelor proiectului de către Ofertant, precum și a perspectivei asupra modului în care acestea pot fi realizate, perimetrul proiectului, delimitarea activităților din afara perimetrului.</p>	<p><i>Specificația tehnică oferită de LogicalPoint răspunde tuturor cerințelor cu privire la serviciile de analiză, consultanță continuă și evaluare a securității cibernetice a sistemelor IT (servicii de scanări de vulnerabilități, consultanță, testare a securității cibernetice din cadrul CNAS).</i></p> <p><i>Metodologia de testare LogicalPoint se aliniază standardelor internaționale de domeniu și este descrisă în Oferta Tehnică LogicalPoint. (conform Anexei)</i></p>	Moldova Standard ISO 9001 ISO 27001 NIST ISC2

			<p>b. Sumar executiv - privire de ansamblu asupra procesului de consultanță, analiză, evaluare, instruire, scanări de vulnerabilități continue și testare în securizarea sistemului informațional CNAS: abordarea sistemică a tuturor serviciilor interdependente în securitatea cibernetică.</p> <p>c. Ipoteze de lucru pentru proiect in general și pentru fiecare etapă sau aspect in parte, după cum se considera necesar.</p> <p>d. Descrierea serviciilor în parte în dependență de scop, aplicabilitate, perioadă și resurse. De asemenea, Ofertantul va descrie pentru fiecare serviciu în parte: obiectivele, principalele activități, precum și instrumentele și mijloacele specifice utilizate pentru a le realiza.</p> <p>e. Răspunsul la cerințele specificate din prezentul caiet de sarcini. in aceasta secțiune, Ofertantul trebuie sa includă toate informațiile tehnice și profesionale care vor îndeplini toate cerințele descrise în Caiet de sarcini. Întru asigurarea unei înțelegeri complete de către Ofertant și Beneficiar a cerințelor și răspunsurilor, Ofertantul trebuie sa ofere răspunsuri detaliate la toate cerințele înaintate. Răspunsurile trebuie sa fie însoțite de dovezi corespunzătoare, documente care sa descrie livrabilele aferente proiectului, explicații, extrase din documentația de însoțire, modele care vor respecta cerințele din prezentul caiet de sarcini, etc, exemple de livrabile aferente etapelor de proiect (plan de proiect, plan de instruire, plan de acțiuni, plan de testare, raport lunar scanări, raport de testare și analiză).</p> <p>f. Descrierea managementul proiectului: - Structura organizatorica a proiectului; - Plan de proiect, care sa conțină abordarea de gestionare a proiectului, inclusiv abordarea de asigurare a calității</p> <p>h. Ofertantul își va asuma răspunderea legalității utilizării instrumentelor folosite în cadrul proiectului și va trebui să prezinte Beneficiarului dovada utilizării legale a acestora dacă va fi cazul.</p> <p>1.3. Oferta financiară 1.3.1. Oferta financiara trebuie sa fie întocmită conform Formularului f. 4.2 "Specificații de pret". Acest proiect este un proiect cu preț fix cu toleranta zero de cost</p>		
--	--	--	---	--	--

			<p>(buget), respectiv solicitări de mărire sau revizuire a prețului nu vor fi admise.</p> <p>1.3.2. Oferta financiară trebuie să fie clar întocmită, care să asigure o bună înțelegere de către Beneficiar în ceea ce privește oferta formulată.</p> <p>2. CERINȚE FAȚĂ DE SERVICIILE ACHIZIȚIONATE</p> <p>2.1. Obiectul achiziției</p> <p>Obiectul achiziției reprezintă contractarea serviciilor de analiză, consultanță continuă și evaluare a securității cibernetice a sistemelor IT (servicii de scanări de vulnerabilități, consultanță, testare a securității cibernetice din cadrul CNAS) care vor include:</p> <ul style="list-style-type: none"> - Scanarea de vulnerabilități conform standardelor internaționale cu instrumente speciale. Analiza vulnerabilităților sistemelor informaționale CNAS (inclusiv din Cloud) și identificarea celor adevărate din cele false. Raportarea către CNAS a vulnerabilităților depistate și recomandările viabile de fixare. Consultanță la fixarea vulnerabilităților și a breșelor de securitate depistate precum și consultanță la aplicarea măsurilor compensatorii de protecție cibernetică. Prin acest serviciu se va asigura identificarea posibilelor vulnerabilități care apar zilnic la nivelul sistemelor de operare, bazelor de date și aplicațiilor software. - Consultanță în securizarea infrastructurii, a Cloud-urilor, a rețelelor WAN, LAN, a elementelor IT, prin analiza eficacității tehnologice a soluțiilor de protecție automatizate, a ecranelor de protecție precum și consultanță la aplicarea cerințelor minime de securitate cibernetică pentru instituțiile de stat. Consultarea continuă conform standardelor internaționale la identificarea anumitor soluții și a produselor necesare securizării sistemului informațional al Autorității contractante. - Testarea practică a angajaților prin diverse tehnici de manipulare la disponibilitatea de a oferi date tehnice interne persoanelor terțe - inginerie socială. - Servicii de teste de penetrare (Penetration testing) a infrastructurii autorității contractante din exteriorul infrastructurii și din interiorul acesteia. Ofertantul va prezenta în 		
--	--	--	---	--	--

			<p>Planul de proiect, vectori de atac reali care ar putea fi aplicați de către persoane necunoscute în scopul sustragerii datelor din cadrul sistemelor informaționale sau subminării securității informaționale.</p> <p>Testele de penetrare reprezintă o modalitate de evaluare a securității unui sistem informatic prin simularea unui atac, prin exploatarea vulnerabilităților existente și cunoscute într-un mod asemănător încercărilor de exploatare realizate de către un atacator, cu diferența ca acestea vor fi efectuate într-un mod etic, cu permisiunea Beneficiarului. Procesul implica o analiza activa a sistemelor informatice pentru orice vulnerabilități existente care ar putea rezulta din configurația inadecvata și din breșe cunoscute sau necunoscute, hardware și software.</p> <p>2.2. Scopul serviciilor prestate</p> <p>2.2.1. Scopul serviciilor enumerate mai sus este asigurarea unui climat funcțional și protejat al sistemului informațional precum și asigurarea cerințelor minime obligatorii de securitate cibernetică pentru instituțiile de stat.</p> <p>2.2.2. Ofertantul trebuie să descrie activitățile ce vor fi desfășurate de acesta pentru a răspunde acestor cerințe. Ofertantul trebuie să prezinte informație despre modul în care intenționează să presteze serviciile solicitate la nivelul cerut, și să le descrie în Planul de proiect.</p> <p>2.3. Cerințele față de servicii</p> <p>2.3.1. Serviciile de scanări de vulnerabilități vor avea ca rezultat o analiză complexă a gradului de pericol a vulnerabilităților și breșelor de securitate din sistemele informatice. Vor fi raportate și examinate de către experții Ofertantului vulnerabilitățile cu pericol sporit de securitate și fiecărei vulnerabilități îi vor fi atribuite recomandări de fixare. Scanarea de vulnerabilități va genera un Raport de vulnerabilități prezentat și explicat în detalii conducerii Autorității contractante.</p> <p>2.3.2. Consultanță în securizarea infrastructurii, a Cloud-urilor, a rețelelor WAN, LAN, a elementelor IT vor asigura o informare continuă despre cele mai noi tehnici și metodologii de securizare precum și analiza de către experții Ofertantului a implementării</p>		
--	--	--	--	--	--

				<p>corecte și setării suficiente a ecranelor de protecție gen firewall la nivel de stații, servere, echipamente de rețea, etc.</p> <p>2.3.3 Testele de penetrare reprezintă o evaluare complexă a securității sistemelor informatice ale Beneficiarului, testând eficacitatea măsurilor de securitate implementate prin simularea unor atacuri informatice. Activitățile echipei de testare se vor baza pe practici de "ethical hacking", iar posturile pe care le va lua echipa va fi mixt alcătuit din următoarele:</p> <p>a. Black box - în această situație echipa de testare nu va cunoaște nici o informație despre sistemele auditate, cu excepția informației de accesare a aplicațiilor (pagini web, adrese IP). Aceasta metoda va fi utilizată pentru testarea infrastructurii externe a Beneficiarului.</p> <p>b. Grey Box – echipa de experți va cunoaște unele informații ce țin de topologia infrastructurii precum și conturi de acces de utilizator (VPN). Testarea din interior a infrastructurii va include minim vectorii de atac în scop de re-evaluare a testului de penetrare precedent.</p> <p>2.3.4. Ofertantul va trebui să utilizeze echipamente și aplicații, și să dețină experiența pentru realizarea de teste de penetrare la nivel de rețea, sistem de operare, baze de date, Cloud și aplicații, inclusiv cele web, acțiuni simulate de negare a serviciului (DoS).</p> <p>2.3.5. Ofertantul va trebui să dețină și să utilizeze echipamente și aplicații dedicate pentru identificarea și obținerea informațiilor despre sistemele informatice ținta, identificarea de vulnerabilități, și formularea unor recomandări de remediere.</p> <p>2.3.6. Ofertantul va trebui să dețină proceduri de lucru conforme standardelor în domeniu, prin care este redus riscul de a afecta sistemele informatice aflate în scopul testării.</p> <p>2.4. Cerințe față de livrabilele proiectului Ca urmare a serviciilor prestate, Ofertantul selectat va oferi cel puțin următoarele livrabile:</p> <ul style="list-style-type: none"> • Plan de proiect; • Plan de scanări și testare; • Planul de acțiuni (SOW - Scope of Work); • Raportul de scanări de vulnerabilități care vor include vulnerabilitățile detectate pe 	
--	--	--	--	--	--

			<p>parcursul, catalogate în funcție de gravitatea lor. Raportul va include:</p> <ul style="list-style-type: none"> - Descrierea vulnerabilităților; - Analiza vulnerabilităților și atribuirea gradelor de pericol; - Recomandări și modalități de remediere; - Consultanță de fixare a breșelor și vulnerabilităților. • Rapoarte de analiză, ce vor conține analiza rezultatelor testelor efectuate prin care se vor identifica și vor fi incluse recomandări de remediere conținând cele mai bune acțiuni/măsuri/metode ce trebuie întreprinse/uate/folosite pentru eliminarea sau micșorarea riscului generat de vulnerabilitățile detectate. <p>Rapoartele furnizate de Prestator vor fi structurate în două părți distincte:</p> <ul style="list-style-type: none"> - partea executiva - partea tehnică. <p>Partea executivă va conține descrierea pe scurt a problemelor și vulnerabilităților identificate și va utiliza metode grafice.</p> <p>Partea tehnică va detalia din punct de vedere tehnic problemele și vulnerabilitățile identificate.</p> <p>Partea tehnica va conține cel puțin următoarele capitole:</p> <ul style="list-style-type: none"> • Sumar executiv; • Obiectivele și scopul evaluării; • Prezentarea metodologiei utilizate in cadrul testării; • Descrierea contextului in care s-a desfășurat testarea; • Detalii despre rețeaua și sistemele evaluate : <ul style="list-style-type: none"> o echipamentele și serviciile active (adrese IP, porturi deschise,) o Tipul , versiunea, statusul actualizărilor aplicațiilor o Sistemul de operare • Prezentarea individuala a vulnerabilităților descoperite, după cum urmează: <ul style="list-style-type: none"> o descrierea vulnerabilității; o catalogarea vulnerabilității; o descrierea tehnica; o analiza severității și probabilității; o calcularea riscului; 		
--	--	--	---	--	--

			<p>o contramăsuri recomandate pentru remediere.</p> <ul style="list-style-type: none"> • Alte detalii și recomandări; • Anexa cu lista testelor de securitate efectuate. <p>Recomandările de remediere a problemelor și vulnerabilităților identificate vor cuprinde cele mai bune acțiuni/măsuri/metode ce trebuie întreprinse/luate/folosite pentru eliminarea sau micșorarea riscului generat de problemele și vulnerabilitățile detectate, precum și, recomandări și propuneri de implementare ale acestora.</p> <p>2.5. Cerințe față de membrii echipei de proiect oferată:</p> <p>Ofertantul (Prestatorul) trebuie să prezinte dovezi că poate pune la dispoziția Beneficiarului pentru executarea contractului de achiziție publică ce face obiectul prezentei achiziții, un număr minim de experți-cheie, cetățeni ai Republicii Moldova, după cum urmează:</p> <p>a. Expert-cheie - Manager de proiect</p> <p>b. Expert-cheie – Expert 1</p> <ul style="list-style-type: none"> - Expert testare securitate infrastructură rețea de diferit tip - Expert testare securitate cloud (public, privat, hybrid) <p>c. Expert-cheie – Expert 2</p> <ul style="list-style-type: none"> - Expert testare securitate sisteme informatice - Expert testare securitate aplicații <p>Ofertantul trebuie să facă dovada îndeplinirii de către experții cheie a următoarelor criterii:</p> <p>1. Expert-cheie nr. 1 - Manager de proiect este responsabil de gestiunea eficientă a proiectului. Experiența în domeniul protecției datelor cu caracter personal constituie un avantaj. Deținător al cetățeniei Republicii Moldova.</p> <p>a. Experiență de cel puțin 5 ani în calitate de manager de proiect pe proiecte în securitate cibernetică.</p> <p>b. Experiență în cel puțin 3 proiecte similare cu proiectul CNAS ca complexitate și arie.</p> <p>2. Expert-cheie nr. 2 - Expert securitate infrastructuri informatice și cloud-uri (LAN, WAN, cloud - Saas, PaaS, IaaS) deține cetățenia Republicii Moldova, responsabil de testarea infrastructurilor IT, infrastructurilor WAN, LAN., a cloud-urilor (public, private, hybride) și asigurarea consultanței continuă de</p>		
--	--	--	---	--	--

			<p>securizare a acestora. Evaluarea și examinarea vulnerabilităților depistate la nivel de infrastructuri IT și cloud. Raportarea și instruirea echipei de administratori IT ai Beneficiarului.</p> <p>a. Experiență de cel puțin 10 ani în domeniul securității infrastructurilor informatice.</p> <p>b. Participarea în ultimii 2 ani ca auditor tehnic sau pen-tester la cel puțin 3 contracte similare în domeniul securității infrastructurilor IT și a cloud-urilor.</p> <p>c. Cunoștințe privind testarea de securitate a cloud-urilor de tip SaaS, PaaS, IaaS din punct de vedere al securității informației, dovedite prin diplome/certIFICATE obținute. (CCSP sau echivalent).</p> <p>d. Cunoștințe privind testarea de securitate a infrastructurilor de rețea din punct de vedere al securității informației, dovedite prin diplome/certIFICATE obținute în urma promovării unui examen practic de penetrare efectivă a unui sistem informatic (CEH Practic, LPT Practic, OSCP sau echivalent)</p> <p>e. Cunoștințe privind procesul de analiză a vulnerabilităților și interpretarea rezultatelor obținute în urma procesului de scanare și testare efectuat conform unei metodologii recunoscute în domeniu, dovedite prin diploma/certificare eliberată de o instituție cu recunoaștere la nivel național/internațional (ECSA sau echivalent).</p> <p>3. Expert-cheie nr. 3 - Expert testare securitate sisteme informatice și aplicații - este responsabil de testarea de penetrare a sistemelor informatice și a aplicațiilor.</p> <p>a. Experiența de cel puțin 10 ani în calitate de expert testare securitate sisteme informatice,</p> <p>b. Participarea în ultimii 2 ani la cel puțin 3 contracte similare ca expert în testarea securității sistemelor informatice,</p> <p>c. Cunoștințe privind testarea de securitate a sistemelor informatice din punct de vedere al securității informației, dovedite prin diplome/certIFICATE obținute (CEH sau echivalent),</p> <p>d. Cunoștințe privind securitatea sistemelor informatice dovedite prin diplome/certIFICATE obținute (CISSP sau echivalent),</p>		
--	--	--	---	--	--

				e. Cunoștințe privind securitatea aplicațiilor informatice dovedite prin diplome/certificate obținute (CSSLP sau echivalent), f. Cunoștințe avansate privind sistemele de operare, baze de date, sisteme de virtualizare dovedite prin diplome/certificate obținute (precum Microsoft/Linux, Oracle, VMWare sa).		
TOTAL						

(Semnat electronic)

Numele, Prenumele: Melnic Ion

În calitate de: Administrator

Ofertantul: LogicalPoint SRL

Adresa: mun.Chisinau str. A.Puskin 5B

Data: 20 august 2024