LOGICALPOINT

Anexa nr.22
din Ordinul MF115/2021

Specificaţii tehnice

Digitally signed by Melnic Ion
Date: 2023.08.20 20:30:41 EEST
Reason: MoldSign Signature
Location: Moldova

Numărul procedurii de achiziţie nr. ocds-b3wdp1-MD-1691562536755 din 9 august 2023

Obiectul achiziţiei: 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)

Denumirea serviciilor	Denumirea modelului serviciului	Ţara de origine	Produ-cătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
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)	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)	R.Moldova	Logical Point	**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)** **Obiectul achizitiei** 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: - Scananea 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	*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). Metodologia de testare LogicalPoint se aliniază standardelor internaționale de domeniu și este descrisă în Oferta Tehnică LogicalPoint. (conform Anexei)*	Moldova Standard ISO 9001 ISO 27001 NIST ISC2

				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 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. Testele de penetrare reprezintă o modalitate de evaluare a securității unui sistem informatic prin simularea unui atac, prin exploatarea vulnerabilităților existente și cunoscute intr-un mod asemănător încercărilor de exploatare realizate de către un atacator, cu diferența ca acestea vor fi efectuate intr-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. **2.2. Scopul serviciilor prestate** 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. 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. **2.3. Cerințele față de servicii** **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. 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 corecte și setării suficiente a ecranelor de protecție gen firewall la nivel de stații, servere, echipamente de rețea, etc. 2.3.3 Testele de penetrare reprezintă o evaluare complexă a securității sistemelor informatice ale Beneficiarului, testând eficacitatea masurilor 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: a. Black box - in aceasta situație echipa de testare nu va cunoaște nici o informație despre sistemele auditate, cu excepția informației de accesare a aplicatiilor (pagini web, adrese IP). Aceasta metoda va fi utilizata pentru testarea infrastructurii externe a Beneficiarului. 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. 2.3.4. Ofertantul va trebui sa 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). 2.3.5. Ofertantul va trebui sa 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.		

				2.3.6. Ofertantul va trebui sa dețină proceduri de lucru conforme standardelor în domeniu, prin care este redus riscul de a afecta sistemele informatice aflate in scopul testării. **2.4. Cerințe față de livrabilele proiectului** Ca urmare a serviciilor prestate, Ofertantul selectat va oferi cel puțin următoarele livrabile: • 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 parcursul, catalogate în funcție de gravitatea lor. Raportul va include: - 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/luate/folosite pentru eliminarea sau micșorarea riscului generat de vulnerabilitățile detectate. Rapoartele furnizate de Prestator vor fi structurate în două părți distincte: - partea executiva - partea tehnică. Partea executivă va conține descrierea pe scurt a problemelor și vulnerabilităților identificate și va utiliza metode grafice. Partea tehnică va detalia din punct de vedere tehnic problemele și vulnerabilitățile identificate. Partea tehnica va conține cel puțin următoarele capitole: • 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 : 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: o descrierea vulnerabilității; o catalogarea vulnerabilității; o descrierea tehnica; o analiza severității și probabilității; o calcularea riscului; o contramăsuri recomandate pentru remediere. • Alte detalii și recomandări; • Anexa cu lista testelor de securitate efectuate. Recomandările de remediere a problemelor și vulnerabilităților identificate vor cuprinde cele mai bune acțiuni/masuri/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. **2.5. Cerințe fată de membrii echipei de proiect ofertată:** 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: **a. Expert-cheie 1** - Manager de proiect **b. Expert-cheie 2 –** - Expert testare securitate infrastructură rețea de diferit tip - Expert testare securitate cloud (public, privat, hybrid) **c. Expert-cheie 3 –** - Expert testare securitate sisteme informatice - Expert testare securitate aplicații Ofertantul trebuie sa facă dovada îndeplinirii de către experții cheie a următoarelor criterii: 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. a. Experiență de cel puțin 5 ani în calitate de manager de proiect pe proiecte in securitate cibernetică. b. Experiență în cel puțin 3 proiecte similare cu proiectul CNAS ca complexitate și arie. 2. Expert-cheie nr. 2 - Expert securitate infrastructuri informatice și cloud-uri (LAN, WAN, cloud - Saas, PaaS, IaaS) deține cetățeania Republicii Moldova, responsabil de testarea infrastructurilor IT, infrastructurilor WAN, LAN., a cloud-urilor (public, private, hybride) și asigurarea consultanței continuă de securizare a acestora. Evaluarea și examinarea vulnerabilităților depistate la nivel de infrastructuri IT și cloud. Raportarea și instruirea echipei de administratori IT ai Beneficiarului. a. Experiență de cel puțin 10 ani în domeniul securității infrastructurilor informatice. b. Participarea în ultimii 2 ani ca auditor tehnic sau pen-tester la cel putin 3 contracte similare în domeniul securității infrastructurilor IT și a cloud-urilor. 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). 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) e. Cunoștințe privind procesul de analiză a vulnerabilităților și interpretarea rezultatelor obținute in urma procesului de scanare și testare efectuat conform unei metodologii recunoscute in domeniu, dovedite prin diploma/certificare eliberata de o instituție cu recunoaștere la nivel național/internațional (ECSA sau echivalent). 3. Expert-cheie nr. 3 - Expert testare securitate sisteme informatice și aplicații **- este** responsabil de testarea de penetrare a sistemelor informatice și a aplicațiilor.		

				a. Experiența de cel puțin 10 ani în calitate de expert testare securitate sisteme informatice, b. Participarea în ultimii 2 ani la cel puțin 3 contracte similare ca expert în testarea securității sistemelor informatice, c. Cunoștințe privind testarea de securitate a sistemelor informatice din punct de vedere al securității informației, dovedite prin diplome/certificate obținute (CEH sau echivalent), d. Cunoștințe privind securitatea sistemelor informatice dovedite prin diplome/certificate obținute (CISSP sau echivalent), 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