Anexa nr. 22
la Documentația standard nr._____

din "____" _____ 2023

Specificaţii tehnice

[Acest tabel va fi completat de către ofertant în coloanele 2, 3, 4, 6, 7, iar de către autoritatea contractantă – în coloanele 1, 5,]

Procedura de achiziție: ocds-b3wdp1-MD-1692622074486 din 21.08.2023						
Obiectul achiziției: *Servicii de testare a securității sistemului informatic TERMOELECTRICA S.A*						
Denumirea bunurilor/serviciilor	**Denumirea modelului bunului/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
Lotul 1. *Servicii de testare a securității și evaluare a vulnerabilităților informatice în cadrul Sistemului Informatic al Termoelectrica SA*						
Servicii de testare a securității și evaluare a vulnerabilităților informatice în cadrul Sistemului Informatic al Termoelectrica SA	Servicii de testare a securității și evaluare a vulnerabilităților informatice în cadrul Sistemului Informatic al Termoelectrica SA	Republica Moldova	ICS Reliable Solutions Distributor SRL	1. **Scopul serviciilor:** • Identificarea riscurilor asociate prin prisma prevederilor standardului SM EN ISO/IEC 27001; • Identificarea aplicațiilor vulnerabile și de risc sporit în rețea, inclusiv cele expuse in internet; • Evaluarea vulnerabilității infrastructurii de rețea inclusiv infrastructura wireless; • Elaborarea recomandărilor și planului de remediere cu măsurile tehnice și operaționale pentru eliminarea/minimizarea riscurilor identificate și evaluate ca cele critice. **2. Obiecte de testare:** Principalele obiecte ale testării sunt: • Infrastructura de rețea (inclusiv echipamente active, routere, comutatoare). • Servere și gazde, inclusiv sisteme de operare și servicii. • Aplicație software utilizată în sistem. • Protocoale de comunicație și servicii de rețea. • Aplicații web. **3. Metode de testare:** Pentru atingerea obiectivelor stabilite se vor aplica cel puțin următoarele metode de testare a securității cibernetice: • Analiză externă (mediul informațional al sistemului, zonele de domeniu etc.). • Scanarea pentru vulnerabilități.	Specificatia tehnica propusa este conform matricei de conformitate prezentate.	

				• Testare de penetrare - folosind instrumente și metode specializate (vezi punctul 7). Vor fi utilizate cel puțin 2 tipuri de teste: - Testele automate – vor identifica erori de programare în aplicațiile utilizate și vor fi efectuate cu ajutorul unor aplicații specializate precum instrumentele de scanare a vulnerabilităților, a aplicațiilor web și a codului, instrumente de testare și identificare a eventualelor erori de programare din aplicații în vederea exploatării lor. - Testele manuale – vor analiza aspectele ale aplicațiilor care necesită intuiția umană, identificând-se erori logice de programare, și vor analiza și confirma sau infirma rezultatele testelor automate. • Analiza codului (dacă este necesar). • Inginerie socială (verificarea nivelului de conștientizare a personalului cu privire la securitate). **4. Lista vulnerabilităților și aspectelor de securitate pentru a fi testate:** • Deficiențe în configurarea echipamentelor de rețea. • Deschiderea de porturi și servicii disponibile în rețeaua externă. • Puncte slabe în autentificare și control al accesului. • Vulnerabilitatea aplicațiilor web • Posibile vulnerabilități de securitate fizică. **5. Planul de testare:** **Va conține minim următoarele faze:** ➢ **Faza de colectare a informațiilor:** • Identificarea scopurilor de testare și formarea unei ipoteze de lucru. • Colectarea de informații despre sistem (domeni IP, domenii, informații despre personal etc.). ➢ **Faza de scanare și de detectare a vulnerabilităților:** • Utilizarea scanerelor de vulnerabilitate pentru a găsi porturi și servicii deschise. • Utilizarea instrumentelor specializate pentru detectarea vulnerabilităților. ➢ **Analiza vulnerabilității si faza de exploatare:** • Încercările de a exploata vulnerabilitățile găsite pentru a obține acces neautorizat. • Analiza rezultatelor încercărilor de exploatare. ➢ **Faza de analiză a securității aplicației web:** • Verificarea aplicațiilor web pentru vulnerabilități precum SQL injection, XSS etc.		

				➢ **Faza de analiză Testarea securității sistemului de e-mail:** • Verificarea vulnerabilităților precum refuzul serviciului (DoS) sau injectarea de cod rău intenționat. • Autentificarea utilizatorului și verificări de autorizare pentru a preveni accesul neautorizat. • Testarea posibilității de interceptare a datelor și analiza traficului pentru a asigura protecția datelor. • Verificarea posibilității de acces la distanță la căsuța poștală prin protocoalele POP3, IMAP, SMTP. **6. Lista instrumentelor pentru efectuarea testelor de penetrare:** *Notă: Lista instrumentelor nu este obligatorie, specificate în termenii de referință și pot fi utilizate altele alternative, care depind de obiectivele specifice ale testării și de caracteristicile obiectelor. Utilizarea fiecărui instrument, trebuie să fie coordonată în prealabil cu proprietarul sistemului/aplicației/rețelei.* **6.1. Scanere de vulnerabilitate:** • **Nmap:** Pentru a scana rețeaua pentru gazde active și porturi deschise. • **OpenVAS:** Pentru a detecta vulnerabilități cunoscute în serviciile de rețea. • **Nessus:** Pentru detectarea vulnerabilităților și analiza securității rețelei. **6.2. Instrumente de analiză a aplicațiilor web:** • **Burp Suite**: Pentru analiza securității aplicațiilor web, interceptarea și modificarea traficului. • **OWASP ZAP:** Un instrument gratuit pentru descoperirea vulnerabilităților în aplicațiile web. • **Sqlmap:** Pentru a automatiza detectarea și exploatarea injecțiilor SQL. **6.3. Instrumente pentru testarea vulnerabilităților rețelei:** • **Metasploit Framework**: Pentru a verifica vulnerabilitățile rețelei și pentru a exploata vulnerabilitățile. • **Wireshark:** Pentru a analiza traficul de rețea și a identifica vulnerabilitățile. **6.4. Instrumente de analiză a securității codului:** • **FindBugs**: Pentru a găsi vulnerabilități în codul Java. • **Bandit:** Pentru a scana codul Python pentru vulnerabilități.		

				6.5. Instrumente pentru analiza rețelelor wireless: • Aircrack-ng: Pentru analiza securității rețelei wireless și cracarea WPA/WPA2 PSK. **7. Restricții** Restricții care pot afecta testarea, cum ar fi: • Fără testare în timpul programului de lucru. • Interzicerea utilizării anumitor instrumente sau metode. **8. Rezultate așteptate:** • Raport asupra testării efectuate cu o descriere detaliată a vulnerabilităților, riscurilor identificate și recomandări pentru eliminarea acestora. • Evaluarea eficacității mijloacelor existente de protecție și de detectare a incidentelor. • Descrierea detaliată a încercărilor reușite și nereușite de a exploata vulnerabilitățile. Raportul de evaluare va conține cel puțin următoarele capitole: - Sumar executiv - Obiectivele și scopul evaluării - Prezentarea metodologiei utilizate în cadrul testării - Descrierea contextului în care s-a desfășurat testarea - Detalii despre rețeaua și sistemele evaluate - Prezentarea individuala a vulnerabilităților descoperite: o descrierea vulnerabilității o catalogarea vulnerabilității o descrierea tehnică o analiza severității și probabilității o calcularea riscului o contramăsuri recomandate pentru mediere - Anexe cu lista testelor de securitate efectuate. **9. Condiții de testare:** • Testarea trebuie efectuată într-un mediu de testare dedicat pentru a evita impactul negativ asupra sistemului de producție. • înainte de testare trebuie sa fie aprobat de beneficiar programul de testare. Testarea nu ar trebui să degradeze performanța sistemului sau să compromită disponibilitatea sistemului.		

Semnat:_____
Numele, Prenumele:Vitalie Bîrsan
În calitate de: Administrator
Ofertantul: ICS Reliable Solutions Distributor SRL

Adresa: str. Alexandru cel Bun 85, Chisinau, MD - 2012

Digitally signed by Bîrsan Vitalie
Date: 2023.08.29 12:15:22 EEST
Reason: MoldSign Signature
Location: Moldova