XONTECH

Specificaţii tehnice (F4.1)

[Acest tabel va fi completat de către ofertant în coloanele 3, 4, 5, 7, iar de către autoritatea contractantă – în coloanele 1,2, 6, 8]

Numărul procedurii de achiziţie:	**ocds-b3wdp1-MD-1602163426198 din 08.10.2020**
Denumirea procedurii de achiziţie:	**Pachete software pentru reţele, internet şi intranet**

Cod CPV	**Denumirea bunurilor**	**Modelul articolului**	**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	8
48200000-0	Lotul nr. 10: Subscripția pentru soluția de scanare a vulnerabilităților de aplicație	**F-Secure Radar Cloud for 25 IP's/host for 1 year of support**	**Finlanda**	**F-Secure**	Cerințe generale: 1. Instrument de scanare a vulenrabilităților de aplicație; 2. Interfața web cu acces prin protocoale securizate; 3. Capacitati de web crawling; 4. Scanari de tip SQL Injection, XSS, CSRF, Malware, etc; 5. Capacități de scanare cu și fără autentificare;	Conform Anexei 1 la formular. Matricea de conformitate	Nu se aplică

					6. Detectarea aplicațiilor web populare și a versiunilor vulnerabile; 7. Detectarea permisiunilor incorecte la directorii și metode HTTP permise; 8. Constructor de requesturi HTTP customizate; 9. Testare la parole slabe; 10. Propuneri de soluții cu privire la mitigarea vulnerabilităților detectate; 11. Rapoarte customizabile în diverse formate (PDF, XLSX, CSV, HTML, etc.); 12. Politici de scanare preconfigurate și customizabile 13. Soluție compatibilă cu mediile virtualizate		

					(VMware vSphere). 14. Număr total de hosturi supuse scanarii – nelimitat. 15. Numar de hosturi scanate simultan – minim 25. 16. Termenul de valabilitate/ garanție: 12 luni		

Semnat:
Nume: **Irina Vicol**
În calitate de: **Administrator**
Ofertantul: **Xontech Systems SRL**
Adresa: str. Alexandru cel bun 85, MD-2012, mun Chisinau, Republica Moldova.
Data: “26” octombrie 2020

XONTECH

Anexa 1

Matricea de conformitate conform cerințelor solicitate in Anexa 1 pentru Lotul 10:

Nr. d/o	Denumirea bunurilor solicitate	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant
		Lotul 10	
1.	Lotul nr. 10: Subscripția pentru soluția de scanare a vulnerabilităților de aplicație	Cerințe generale: 1. Instrument de scanare a vulenrabilităților de aplicație; 2. Interfața web cu acces prin protocoale securizate; 3. Capacitati de web crawling; 4. Scanari de tip SQL Injection, XSS, CSRF, Malware, etc; 5. Capacități de scanare cu și fără autentificare; 6. Detectarea aplicațiilor web populare și a versiunilor vulnerabile; 7. Detectarea permisiunilor incorecte la directorii și metode HTTP permise; 8. Constructor de requesturi HTTP customizate; 9. Testare la parole slabe; 10. Propuneri de soluții cu privire la mitigarea vulnerabilităților detectate; 11. Rapoarte customizabile în diverse formate (PDF, XLSX, CSV, HTML, etc.); 12. Politici de scanare preconfigurate și customizabile 13. Soluție compatibilă cu mediile virtualizate (VMware vSphere). 14. Număr total de hosturi supuse scanarii – nelimitat. 15. Numar de hosturi scanate simultan – minim 25. 16. Termenul de valabilitate/ garanție: 12 luni	**F-Secure Radar Cloud for 25 IP's/host for 1 year of support:** An enterprise vulnerability scanning and management solution hosted in the Cloud. Subscription includes unlimited scans of any type in Radar (Discovery, System- and Web Scan) and maintenance and support services for 12 months. **Key concepts and components:** **Vulnerability scans:** Vulnerability scans test systems or web applications within your network for vulnerabilities that could be exploited in a cyber attack. Radar includes two separate types of vulnerability scan: system scan and web scan. **Scan groups:** In Radar, all vulnerability scan targets are stored in logical containers called scan groups. Each scan group can contain both system scans and web scans. **Scan templates:** Scan templates allow you toeasily create severalscans, eachofwhich can apply toa specific scenario or part of your network, but share a number of settings. You can create templates for each scan type (discovery scan,systemscan, andweb scan) aswell asscheduling templatesthat can be applied to any scan. **Discovery scan:** System scan is a network-based vulnerability scanner that is able to scan any system with an IP for common vulnerabilities. System scan's vulnerability detection is based on both active and passive vulnerability checks. For example, it will attempt to identify the service (product) and its version number.

			Once identified, the system scan checks if that particular software has any known vulnerabilities. In addition to passive scanning based on banner grabbing, system scan also runs active checks in an attempt to confirm the existence of certain vulnerabilities or system misconfigurations. It can also identify missing security patches and outdated software if authenticated scanning has been enabled. Note: System scan is non-disruptive and designed not to cause Denial of Service conditions on your systems. **Web scan**: allows you to scan and test web applications. You can use web scans during the development of new applications as part of the development life cycle. This results in being able to uncover vulnerabilities faster, thus significantly reducing the cost and amount of resources required to mitigate vulnerabilities at a later stage, as security issues are caught very early in the process. Web scan is considered an additional scanning feature that can be applied on top of an existing system scan. In other words, it is recommended that whenever you scan a target with a web scan, it should also be scanned with system scan **Internet discovery:** Internet discovery allows you to collect data on public systemsthrough crawling and portmapping. You can use this to find your organization's Internet-facing systems and add them to scan groups for vulnerability scanning. **Authenticated Scanning:** In addition to regular network-based scanning,where the host's ports are scanned and the exposed services are reviewed forflaws, you can alsorun a systemscan in authenticated mode,which enables it to authenticate the target host. Authenticated scanning helps the scanner eliminate potential false positives and check patch levels and other misconfigurations. **Scan node:** A Radar scan node is a server on which you can install one or more scan engines. Radar has three different scanning engines: discovery, system, and web scan. You can attach an

			unlimited number of scan nodes to the Radar Security Center. You may need multiple scan nodes if you have several network segments or need additional scanning power. Radar Security Center: The Security Center is the core component of the whole F-Secure Radarsolution. It is aweb-based interface where you can manage (start and stop)scans, browse vulnerabilities, create reports, and much more. • F-Secure Radar reprezintă soluția ce vă permite să rulați scanarea de descoperire a rețelei și scanarea porturilor, scanări ale vulnerabilității platformei și scanări ale aplicațiilor web. • Portalul către soluția F-Secure Radar se acceseaza securizat prin protocolul HTTPS. Toate metadatele, fișierele și alt conținut sunt transferate în siguranță folosind criptarea TLS 1.2. • Solutia F-Secure Radar utilizează accesarea cu crawling și port mapping pentru a vă permite să colectați date pe sisteme publice. Puteți căuta date pe bază de locație, domeniu de nivel superior, pay-level domain, cuvinte cheie, nume de gazdă și adresă IP. • F-Secure Radar permite scanarea fara autentificare si cu autentificare: • Windows credentials (WinRM) • Linux credentials • Windows credentials (RPC) • Radarul detectează configurarea greșită a securității. Funcția Rulează cu un atac în verificările de scanare web și utilizează injecția de comandă / injecția de comandă oarbă (GET, POST, COOKIE, HEADER) pentru a găsi

			vulnerabilități. Mai jos este lista categoriilor WASC care sunt acoperite de Web Scan: - WASC Categories coverage: - WASC-04 Missing Encryption of Sensitive Data - WASC-05 External control of file name or path - WASC-05 Remote file inclusion - WASC-08 Cross-site scripting - WASC-12 Content spoofing - WASC-13 Private IP address leakage - WASC-13 Execptions and Errors - WASC-14 Cacheable HTTPS response - WASC-14 Insecure cookie attributes (Missing httpOnly/Secure cookie attribute) - WASC-15 ASP.NET ViewState without MAC enabled - WASC-16 Directory Browsing Enabled - WASC-19 SQL injections - WASC-22 Improper Output Handling (Inside HTTP Headers) - WASC-25 Improper Neutralization of CRLF Sequences in HTTP Headers - WASC-31 Blind command injection - WASC-31 Command injection - WASC-34 Predictable Resource Location - WASC-38 Open redirection - WASC-42 File upload functionality detected • Este posibil să adăugați antet de solicitare HTTP personalizat în configurația de scanare Web. • F-Secure Radar detectează parole slabe și implicite pentru diferite servicii precum: Ciscoo SSH , Glassfish server, HP Management Utility, MongoDB, Oracle DB, Oracle Enterprise Manager, PCAnywhere, Sitecore, Solarwind Virtualization

			Manager, SNMP (v1, v2), Splunk, VMWare ESX, Fortinet Fortios SSH, HTTP login with any credentials, Informix, MSSQL, MySql, Postgres, SMB, solidDB, Tomcat, SSH, VNC, Wordpress • F-Secure Radar oferă soluții de remediere a vulnirabilitaților detectate. • F-Secure Radar oferă rapoarte customizabile in format: CSV , DOCX , XML. • F-Secure Radar ofera politici de scanare preconfigurabile si customizabile. • Soluția F-Secure Radar se instalează pe o mașină virtuală pe Windows Server 2008 R2 or newer (full installation, not Server Core).EXE sau pe Ubuntu Linux (16.04 LTS or 18.04 LTS version). • Nr nelimitat de scanari si Scan Nodes supuse scanarii in limita volumului licenței. • Numar de hosturi scanate simultan - 25 IP. • Termenul de subscriptie inclus pentru 12 luni. Alte detalii suplimentare despre solutia propusa poate fi gasita in datasheet anexat si pe acest link: https://www.f-secure.com/en/business/solutions/vulnerability-management/radar