International Organization for Migration (IOM)
The UN Migration Agency

Section I
Terms of Reference

Services Requirements

Vulnerability Management Solution

These Terms of Reference were developed by the International Organization for Migration to request for proposals (RFP) from qualified vendors to deliver a risk-based ***Vulnerability Management*** solution to provide asset discovery, vulnerabilities identification and classification, prioritization, and customizable reports for **24,500 assets** distributed through 400 offices connected through a wide-area network and the Internet.

1. Organization Background

Established in 1951, the International Organization for Migration (IOM) is an international intergovernmental organization that recently joined the United Nations system. With over 160-member states and offices in more than 150 countries, the breadth and depth of IOM's work reflect a level of experience and expertise in providing migrant services unmatched in the international community. IOM provides advice and services to governments to promote the principle that humane and orderly migration benefits migrants and society.

IOM works with its partners in the international community to meet the growing operational challenges of migration, advance understanding of migration issues, encourage social and economic development through migration, and uphold the well-being and human rights of migrants. IOM works to help ensure the orderly and humane management of migration, promote international cooperation on migration issues, assist in the search for practical solutions to migration problems, and provide humanitarian assistance to migrants in need, including refugees and internally displaced people.

IOM provides its services through a worldwide network of more than 400 field locations in more than 150 countries, including 9 Regional Offices, the Head Quarters in Geneva, and 2 Administrative Centers located in Panama and Manila, which provide core support in the areas of information technology, finance, human resources, and other administrative services to IOM's network of offices.

2. General Requirement

The ***Vulnerability Management*** solution must be a SaaS platform (cloud-based solution) that provides real-time (agent and agentless) and on-demand vulnerability assessments, offering asset discovery, automated continuous monitoring, prioritizing findings based on risks associated, and the capability to generate custom reports of detected vulnerabilities.

The complete solution and delivery of the services must include all required software/licenses (3-years subscription) and the cost for the support during the initial deployment (propose a deployment design based on IOM architecture) and during the configuration of the automated and third-party integration; and any recurring cost. No additional cost to IOM not included in this financial proposal will be accepted to implement the project successfully.

The proposal must consider a universe of **24,500 assets** to be scan (including workstations, cloud, and on-prem servers, web servers, corporate applications, firewalls, network devices, and containers/images), distributed on cloud on-prem environments.

It is expected that the solution has a modular design providing IOM the option to expand and acquire additional functionalities without affecting the deployed scenario; for example, Web Application Scanning and Automated Remediation / Patching modules (including integrations with Microsoft Azure Intune) for a future expansion to leverage up the IOM's vulnerability and patch management capabilities, and vulnerability scanning capabilities to the Internet of Things (IoT) devices.

3. Scope of Work & Deliverables

The Service Provider shall provide the required licenses and administrative access for a 3-years subscription to the SaaS-based Vulnerability Management main portal and additional modules (if applicable) to fulfill the obligations necessary to complete the project implementation.

The Service Provider shall assist / support during the initial deployment (propose a deployment design based on IOM architecture) and during the configuration of the automated and third-party integration. Additionally, the service provider must provide knowledge transfer and training to enable IOM in-house staff to manage the product daily.

The service provider shall submit to IOM user documentation in the English language.

4. Mandatory Technical & Functional Requirements

The proposed solution must achieve several important criteria, including but not limited to:

Technical Requirements

Criteria	Requirement
Vulnerability Coverage	> 40,000 CVEs (vulnerabilities)
Scanning Accuracy	Six Sigma 99.99966% accuracy (False-Positive Rate below 0.00034%)
SaaS Uptime	SLA level: 99.95 % uptime/availability
Data Security	SSL/TLS 1.2 Encrypted Connections; AES-256 Encrypted Stored Data

Functional Requirements

Criteria	Requirement
SaaS Centralized Management	Centralized cloud-based Vulnerability Management solution to eliminate siloed data: consolidating, storing, and filtering all vulnerability scan data into a common repository. The platform must role-based access control and the creation of several users (analysts).

Multi-Platform Capabilities (including image/container-based vulnerability analysis)	The solution must be able to run internal and external vulnerability assessment scans using local credentials, domain credentials, or un-credentialed vulnerability discovery and receive specific remediation suggestions from around 24,500 assets distributed as (in the cloud and on-prem environments): • approximately 22,000 workstations (desktop and laptops) including Windows, Linux, and Mac OS operating systems; with multiple software installed (Adobe, SAP, Microsoft, etc.); • over 1400 worldwide servers: physical, virtual (e.g., VMware, ESXi, Hyper-V) and cloud-based (e.g., AWS, Azure); working on various platforms, including Windows and Linux operating systems (including database servers: Oracle, MS SQL Server, MySQL) • around 400 firewalls, including Cisco, Palo Alto, and FortiGate equipment and networks devices • around 350 websites (most of them are Drupal) • around 350 containers' images (Kubernetes)
Asset Discovery & Inventory	Creates an inventory of the assets across the network, identifies the vulnerabilities of the various elements of the technology stack and stays current on breaking threat alerts.
Reachability	Have the possibility to assess assets hosted in any infrastructure, including assets behind firewalls, assets in an office without a firewall, and assets located in the DMZ network.
Auto-Tagging / Asset Grouping	Grouping assets based on locations in important for IOM reports, so it is crucial that the solution offers asset grouping capabilities and/or automatic tagging options for assets. These tags should be invoked in dashboards, queries, filters, reports, and other functions of the solution.
Analytics-Driven Prioritization	Automating the analysis of the vulnerabilities to focus on the critical risks to avoid investing the time inappropriately on low-risk exposures. The idea is to have a short list of action items that can be executed quickly to eliminate the risk of exploitation by attackers.
Continuous Monitoring	Establish repeatable and schedulable workflows to track, monitor easily, and remediate security vulnerabilities over time, to prevent potential cyberattacks and data breaches. It must be able to find the open ports and existing services across a network. Indicate if a detected vulnerability is exploitable using Metasploit, CANVAS, CORE, etc.
Performance	Realize optimal performance via non-intrusive scanning, without impacting availability or performance and within a limited time frame. The solution should offer low bandwidth, non-disturbing, and agentless scans. The application should support concurrent scan tasks and scheduled scans.
Traceability	The solution must provide a history of all the actions that involved a particular asset (timelines).
Configuration Assessments	The application must examine the operating systems for misconfiguration, discover wireless and wired networks and devices to identify insecure and vulnerable configurations based on CIS Benchmarks.

	Additionally, it must be able to scan the configuration of cloud infrastructure solutions like AWS and Azure.
Filtering Options	It provides multiple filtering options such as exploitability, malware, dates, severity/criticality, a module that detected it (active, passive scanner, agent, cloud connector), and others.
Customizable Reporting	Allow IOM to generate customizable reports (e.g., XML, CSV, XLS, PDF, HTML) not only for technicians but also for stakeholders and executives through relevant reports and graphs (dashboards). The report must be able to include hostname (NetBIOS, DNS), not only IP addresses.
Remediation Guidance	The solution must provide dynamic remediation reports based on asset groups to easily assign to the teams responsible for those assets, generating email notifications of scan results and remediation recommendations (concise, actionable, and clear step-by-step instructions).
Automation	Streamline analysis through the resolution process with automated prioritization, ticket creation, and reporting.
Third-party integration	API connections manage assets, scans, reports, remediations, and tickets, with third-party solutions as IBM QRadar SIEM, Azure Sentinel, Microsoft Intune / SCCM, Freshservice, etc.; including integration with reporting tools as Power BI.
Access Security	Multiple user access model must support role-based access control (RBAC) principles. Security analysts must be able to view other analysts' scans and results as a centralized solution.
Licensing	3-years renewable subscription; based on the number of assets or websites/web apps, not limited to the number of executed scans (unlimited number of scans).
Vendor Support	For any product purchased, most especially for systems security, timely and relevant vendor support is important. Service providers must have relevant expertise in Vulnerability Management solutions and support your company's short-term and long-term plans.
Vendor Experience	It is recognized by industry analysts as the leaders in vulnerability-based risk management.
Maturity	The software must have been on the market since 2015 or earlier.

5. Desired Requirements

Criteria	Requirement
Integration with Password Vaults	Secure connection to password vaults solutions.
SLA Definitions	Define compliance goals/milestones for a period (as vulnerabilities remediation projects).
CI/CD Pipeline Integration	Capable of being integrated with Amazon AWS and/or Microsoft Azure CI/CD pipelines.

6. Service Level Agreement (SLA)

- The service provider shall provide support on 24x7x365, supporting or solving issues via email, portal, chat or phone support and give a set of action plans within (2) hours from the receipt of reported issues.
- The service provider shall provide software maintenance on an annual basis, including software upgrades, patches, and bug fixes.