International Organization for Migration (IOM)
The UN Migration Agency

Section I
Terms of Reference

Services Requirements

Dynamic Application Security Testing (DAST) Solution

The Terms of Reference were developed by the International Organization for Migration to request for proposals (RFP) from qualified vendors to deliver a risk-based ***Dynamic Application Security Testing (DAST)*** solution to provide asset discovery, vulnerabilities identification and classification, investigation of running applications to verify exploitability of security vulnerabilities, vulnerabilities prioritization, and customizable reports for 350 websites worldwide distributed on cloud and on-prem environments.

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 that are 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 migrants' well-being and human rights. IOM works to help ensure the orderly and humane management of migration, promote international cooperation on migration issues, assist in searching 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 ***Dynamic Application Security Testing (DAST)*** solution must be an agentless (no application’s instrumentation needed) SaaS platform (cloud-based solution) that provides real-time web sites/web application security assessments, offering asset discovery, automated continuous monitoring, prioritizing findings based on risks associated, investigating running applications to verify the exploitability of security vulnerabilities, and the capability to generate custom reports of detected vulnerabilities (executive, per asset group, per vulnerability).

The complete solution and delivery of the services must include all required software/licenses (3-years subscriptions) 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 (minimizing human interaction time in workflows); 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 **350 websites** worldwide distributed on cloud and on-prem environments.

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 Dynamic Application Security Testing (DAST) main portal 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
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
Concurrent Scans	At least 5 concurrent scans (parallel scans); unlimited is preferred

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	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 350 websites/web applications worldwide distributed (in the cloud and on-prem environments), developed in different scenarios (e.g., Drupal, .NET)
Websites Discovery & Inventory	Creates an inventory of the websites 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 important for the IOM's report; it is crucial that the solution offers asset grouping capabilities and/or automatic tagging options for assets. These tags should allow IOM to invoke them 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).
Web App Deep Scanning	Coverage of over 100 generic vulnerabilities, such as SQL injection and cross-site scripting (XSS), with a great performance against all vulnerabilities in the OWASP top 10. Support authenticated complex and progressive scans. With programmatic scanning of SOAP and REST API services.
Web App Crawler	To map content and functionality, automatically handling sessions, state changes, volatile content, and application logins.
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.
Proof-of-Exploit	Evidence of the exploitable vulnerabilities. If not, at least a confidence level to reduce false positives.
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	Reduce manual/human interaction. 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 websites/web apps, not limited to the number of executed 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	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.
Agentless Scan	The solution should work without the need to instrument the application (agentless deployment); nevertheless, agents to analyze internal resources from the SaaS solution are accepted.

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 into Amazon AWS, Microsoft Azure, and/or Jenkins CI/CD pipelines.
On-Demand Scan Services	The provider should facilitate on-demand scans services based (e.g., MAST on-demand)
Reporting	The solution should generate compliance reports based on the main 'web security industry standards': OWASP Top 10, WASC Threat Classification, CWE/SANS Top 25. Additionally, it should be able to generate 'regulatory' compliance reports.
Scanning Capabilities	As nice to have, the tool should change behavior to scan REST API, mobile, and containers, without affecting the final financial proposal, considering the main goal of the current RFP is obtaining a DAST.

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.