CONSULTANCY - TERMS OF REFERENCE

UNRWA is a United Nations agency established by the General Assembly in 1949 and is mandated to provide assistance and protection to a population of some 5 million registered Palestine refugees. Its mission is to help Palestine refugees in Jordan, Lebanon, Syria, West Bank and the Gaza Strip to achieve their full potential in human development, pending a just solution to their plight. UNRWA's services encompass education, health care, relief and social services, camp infrastructure and improvement, microfinance and emergency assistance. UNRWA is the largest UN operation in the Middle East with more than 30,000 staff. UNRWA is funded almost entirely by voluntary contributions.

Consultant – DevSecOps Specialist, (Local)

BACKGROUND

UNRWA has signed a Memorandum of Understanding (MoU) with United Nations International Computing Center (UNICC) that aims to enhance livelihood and human development opportunities to Palestine refugees in Gaza. By this new collaboration, UNRWA becomes a provider of Information Management, Technology services and capacity augmentation to UNICC technical team, on a cost recovery basis through IMTD/IT Service Center (ITSC) in HQ-Gaza.
United Nations International Computing Center (UNICC) is a UN agency that provides IT services to other UN agencies on a cost recovery basis.

UNRWA Information Management and Technology Department (IMTD) is seeking a **DevSecOps Specialist** who will work within the Cyber Security Section, the incumbent will be responsible to empower developers and project teams to solve security problems and make application security elastic, agile and focused. This is an opportunity to make a big impact and get lots of ownership. We are looking for someone who thrives in the very early stages of a project and is self-driven.

The consultant will report administratively to Head Information Technology Service Centre at Headquarter Gaza and technically to United Nations International Computing Center (UNICC).

DESCRIPTION OF DUTIES AND RESPONSIBILITIES

- Guide and train developers and project teams to solve security problems;
- Make application security elastic, agile and focused;
- Move automated security into the CI/CD pipelines;
- Monitor attacks the same way performance is monitored in operations;
- Provide help on Security Matters for DevOps team;
- Support diverse environment that has customer facing applications and large-scale data;
- processing infrastructure and APIs
- Collaborate with others on project team or across other project teams;
- Implement continuous integration, continuous (CI/CD) delivery pipeline to limit manual testing and troubleshooting;
- Analyze user interfaces, maintain hardware and software performance tuning, analyze workload and computer usage;
- Maintain interfaces with outside systems, analyze downtimes, analyze proposed system modifications, upgrades and identification of new commercial off the shelf software;
- Identify issues with current software then develop system requirements and program specifications to upgrade or improve existing software;
- Coordinate closely with programmers to ensure proper implementation of program and system specifications and requirements;
- Provide other ad hoc support as required.

MINIMUM QUALIFICATIONS AND EXPERIENCE

- A university degree from an accredited educational institution in Computer Science, Information Technology, or related discipline;
- Minimum of five years of experience in software development including Web applications and technologies; of which a minimum of three years in Cyber Security and cloud security;

- Expert level experience in application and security testing technologies including static code analysis and dynamic analysis;
- Experience with CI/CD tools, including Atlassian, GitLab, Jenkins, Terraform, Puppet, Artifactory, Ansible, and Vagrant;
- Experience in integrating an Identity and Access Management (IdAM) solution into infrastructure and Web applications;
- Experience in integration with SONAR, Veracode, and Security Testing tools like AppScan, Fortify etc.
- Experience with automation/configuration management using either Puppet, Chef or an equivalent
- Familiarity with API Security, Container Security, AWS Cloud Security, Azure DevOps;
- Experience in architecting Cloud solutions which span storage, security, networking and compute capabilities;
- Knowledge and experience with attack simulation, vulnerability management and application testing using automated and manual tools;
- Ability to work with APIs and Plugins to integrate security tools into established CI/CD pipeline;
- Fluency in spoken and written English.

COMPETENCIES

- Applying technical expertise;
- Ability to interact directly with a System Engineering team/Lead, application developers, security specialist and project coworkers and teammates.
- Excellent planning and organizing skills;
- Ability to work well independently and in a collaborative team environment to meet required schedules and timelines;
- Possess outstanding skills in communicating complex technical issues and in providing comprehensive written, oral and/or digital products (including document organization and technical writing). Ensures that information is shared;
- Strong analytic skills and the ability to apply these skills in a multi-tasking environment where more than one project at a given time;
- Ability to learn new concepts and technologies quickly;
- Strong ability to drive for results, to manage and deliver against multiple priorities on time; and committed to achieving outcomes
- A strong troubleshooting methodology and the ability to work under fast-paced timelines with creative solutions paramount.

DESIRABLE QUALIFICATIONS

- Knowledge of threat modelling and risk assessment techniques.
- Up-to-date knowledge of cybersecurity threats, current best practices and latest software.
- Capability to prepare security vulnerability and risk management reports for management.
- Comprehension in the security areas of Key Management Systems, Certificate Management, Encryption, Penetration Testing, Vulnerability Scanning, Security and Monitoring tools, etc.
- Demonstrated background in deploying highly secure solutions
- Preference for one or more of the following certifications; Microsoft Azure Solutions Architect, CCNA Cloud, CCSP, AWS Solutions Architect

CONDITIONS OF SERVICE

- The duration of the consultancy is 6 to 11 months, extendable according to performance and availability of funds.
- Remuneration for this consultancy will depend on the qualifications and relevant experience as follows:
    - Cluster A: $1,600.
    - Cluster B: $1,800.
- The incumbent can be in any of UNRWA fields of operations (Gaza, Jordan, Lebanon, Syria, or West Bank).

APPLICATION PROCESS

Applicants should submit a cover letter and CV or UN Personal History Form demonstrating clearly the knowledge and experience required to meet the consultancy requirements via **consultancy@unrwa.org** indicating the title of this consultancy "**DevSecOps Specialist"** in the subject line of the message and field (area)/country of the candidate. The deadline for the submission of applications is **31 January 2021**.

UNRWA is an equal opportunity employer and welcomes applications from both women and men. UNRWA encourages applications from qualified women. Only those applicants shortlisted for interview will be contacted. UNRWA is a non-smoking environment.

12/01/2021