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 – Cyber Security 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 **Cyber Security Specialist** to work on UNICC consultancy services. The incumbent will be responsible to design, architect, install and manage all technologies such as Security Information and Event Management (SIEM), Malware Information Sharing Platform (MISP), Malware Sandbox, threat hunting tools etc., infrastructure including but not limited to implement new use cases, troubleshooting and optimization. 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

The consultant will work under the guidance and supervision of the Security Operations Centre (SOC) Manager and in close collaboration with other CPI teams. S/he will be responsible of the following duties:

- Install, maintain and troubleshoot the CSOC infrastructure including optimization of logs ingestion, regular maintenance and access controls management;
- Drive the technical onboarding of new clients on the CSOC technologies, including but not limited to initial assessment and quarterly improvement review process;
- Support onboarding and maintenance of a wide variety of data sources to include various OS, appliances, applications and cloud logs;
- Support the creation of new dashboards and applications to enhance visualization of logs;
- Translate customer requirements in SIEM technical implementations;
- Identify and remediate any issues as they arise with SIEM data ingestion;
- Develop, maintain and customize scripts for manipulation of multiple data sources to support customer monitoring requirements;
- Proactively identify, document and implement SIEM enhancements;
- If required, coordinate with clients and internal teams the changes related to SIEM;
- Act as Subject Matter Expert for any SIEM activity.

MINIMUM QUALIFICATIONS AND EXPERIENCE

- A university degree from an accredited educational institution in Computer Science, Information Technology, or related discipline;
- Minimum 5 years of experience in Security Operations Centre; Of which three years related to the following fields:
    - Leading or conducting security incident response activities

    - Reviewing raw log files, data correlation, and analysis (i.e. firewall, network flow, IDS, system logs)
- Employment history must demonstrate increasing levels of responsibility;
- Experience integrating network security/system security related events within security incident event management tools (SIEMs);
- Expert knowledge of SIEM tools including but not limited to Splunk, ELK;
- Excellent understanding of SIEM concepts such as correlation, aggregation, normalization, and parsing;
- Excellent understanding of Cyber Security Operations;
- Sound knowledge of management of cloud-based infrastructure (e.g. Azure, AWS);
- Excellent Linux Administration skills;
- Experience in using scripting languages to automate tasks and manipulate data. Programming experience is a plus;
- Experience integrating solutions in a multi-vendor environment;
- Any of the following certifications: CSIS, CISSP, CEH, CSTA, CSTP, GCFE, OSCP/E, CPP, GCIH, GCIA, CCSP, CISA, Splunk Enterprise Data Administrator, Splunk Enterprise System Administration, Splunk Fundamentals, GMON;
- Fluency in spoken and written English;
- French beginner knowledge is desirable.

COMPETENCIES

- Teamwork: Develops and promotes effective relationships with colleagues and team members. Deals constructively with conflicts;
- Communication: Expresses oneself clearly in conversations and interactions with others; listens actively. Produces effective written communications. Ensures that information is shared;
- Respects and promotes individual and cultural differences: Demonstrate the ability to work constructively with people of all backgrounds and orientations. Respects differences and ensures that all can contribute;
- Produces and delivers quality results. Action oriented and committed to achieving outcomes;
- Moves forward in a changing environment: Open to and can propose new approaches and ideas. Adapts and responds positively to change;
- Builds and promotes partnerships across the Organization and beyond: Develops and strengthens internal and external partnerships that can provide information, assistance and support to ICC. Identifies and uses synergies across the Organization and with external partners.

DESIRABLE QUALIFICATIONS

- 5 years of experience in one or more of the following fields:
    - System administration
    - Network administration
    - Software development
    - Managing cloud-based infrastructure (like Azure, AWS etc.)
    - Implementing and designing Microsoft Active Directory services
- Expert knowledge of Azure Sentinel;
- Understanding of GCP (Google Cloud Platform);
- Expert knowledge of Security Incident Response activities;
- Expert knowledge of EDR solutions (e.g. Windows Defender ATP, Crowdstrike or RedCloak)

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 "**Cyber Security 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