Gonzagagasse 1, 5th floor
A-1010 Vienna
T: +43 1 504 46 77 - 0
F: +43 1 504 46 77 - 75
procurement@icmpd.org
www.icmpd.org

Call for Expression of Interest

Security Operation Center (SOC)

Contents

1 Overview 2

2 Call for Expression of Interest 2
2.1 Enquiries 2
2.2 Procurement process overview 2
2.3 Review and selection 3

3 Qualifications Review Criteria 3
3.1 Mandatory criteria 3
3.2 Solution components 5
3.3 Solution overview 5

4 Submission 6

1 Overview

This Call for Expression of Interest (CEoI) is to be used for pre-qualifying companies (the first stage of the procurement process) to participate in a subsequent Invitation to Tender (ITT) (the second stage of the procurement process).
ICMPD wishes to invite your company to participate in this CEoI for the acquisition of Information security tools and services as per the requirements listed here below.
You are kindly requested to submit your proposal by October 7th 2019 17:00 (Vienna Local time) to procurement@icmpd.org. ICMPD reserves the right to accept or reject all or any part of the proposal submitted.
Late submissions shall be disqualified.
Based on the CEoI responses review, ICMPD intends to issue an ITT to Qualified companies for provision of the required services.

2 Call for Expression of Interest

The expected scope of work is to monitor the client environment and publicly available data in order to detect, analyze and identify possible threats. ICMPD intention is to choose the best systems and services that will meet client's requirements and demonstrate the ability to adjust with the environment growth and changes for many years to come.

2.1 Enquiries

All enquiries related to this CEoI are to be directed to the contact person at procurement@icmpd.org. Information obtained from any other sources shall not deemed official. All questions/answers shall be recorded and depending on its nature, shall be shared with the business community.

2.2 Procurement process overview

The procurement process for this project involves two phases:

- Phase one, consisting of this CEoI to be responded to with an CEoI Submission
- Phase two, consisting of an Invitation to Tender (ITT) inviting formal tenders relating to the project to be submitted.

The following timetable provides an overview of the procurement process main components for this project. It should be noted that successful participation in Phase one is a mandatory requirement for continued participation in the process.

Phase One	
Components	**Date (DD/MM/YY)**
Date of CEoI distribution	**16/09/2019**
Deadline for submission of bidder's questions to CEoI	**23/09/2019**
Expected date for answers to bidder's questions	**30/09/2019**
CEoI submission deadline	**07/10/2019**

Late responses shall not be accepted. CEoI Bidders should note that the high-level description of the project and the ITT set out in this CEoI represents ICMPD's present approach and is subject to final determination at a later date. A full description will be included in the RfP.

2.3 Review and selection

The qualifications review committee will check the documents and responses against the mandatory criteria. Bidders not meeting all mandatory criteria shall be rejected.

3 Qualifications Review Criteria

3.1 Mandatory criteria

The following list of prerequisites is mandatory. Failure to meet them implies the non-eligibility of the bidder to qualify for the ITT [1]*. Bidders can be a single company, a consortium of companies, or a system integrator with international vendors.*

Prerequisites:

1. The bidder shall have a minimum of three years proven of experience in implementing and managing a SOC.

[1] Meeting all the requirements does not necessary yield qualification. This will be subjected to multiple factors such as the number of applications, security clearance, · · ·.

2. The bidder shall have implemented at least six SOC projects in middle to large enterprises including defense and law enforcement agencies. The bidder shall provide a list of references including organizations' sectors; implementation scales (number of devices and contact persons).
3. The bidder should have been providing onsite SOC services with the proposed SIEM tool to at least two BFSI/Telecom/PSU/Government organizations.
4. The bidder should have experience of more than 10 years in providing security services and must have a global presence.
5. The bidder shall have a local presence in Lebanon to provide, among other things, timely and adequate support during the implementation and after the delivery of the project. Proof of local presence is required.
6. The bidder shall provide all related information of the company (or companies in case of a consortium). Commercial registration, copy of vendor agreements, organizational charts, ⋯).
7. The bidder shall provide all the necessary financial information showing sufficient resources to undertake the SOC project (balance sheets and turnover for the last three years)
8. The bidders shall list the cybersecurity profile of its company including the technical and professional ability (total number of employees, number of employees familiar with the project, degrees, certifications and years of experience, CVs). The bidder must have resources certified on industry and product based certifications e.g. ITIL, CISA, CISSP, SIEM certification, CEH or similar. The bidder must have a minimum of four experienced individuals per solution in Lebanon with prior experience in implementing cybersecurity solutions in Lebanon.
9. The bidder's organization should have ISO 27001 certification or any other similar equivalent certification.
10. The bidder should have the capability to provide a 24*7 L1/L2/L3 support.
11. The bidder must accept to sign a Non-Disclosure Agreement (NDA) with the customer in case it is qualified to the second round (see attached template for the NDA).

12. The bidder should be capable of providing the SOC room fit-out including all needed physical equipment.
13. In case of qualification to the second round, the bidder shall accept to conduct a Proof of Concept (PoC) based on the customer's requirement.

3.2 Solution components

In what follows, we list an extended list of the project's components. The listed components might be subject to changes in the ITT. The bidder shall provide a detailed list of all the technology that it will be offering in response to the below needs.

Solution features:

ICMPD wishes to implement a SOC solution that has, but no limited to, the following capabilities:

1. Log collection, management, and integration (aggregation, filtering, connectors…).
2. Real-time correlation based on pre-defined use-cases (built-in, user-defined…); the system must be able to re-run use cases on past collected events.
3. Vulnerability management tools.
4. Threat feeds, threat intelligence and hunting solutions.
5. Deception techniques and technologies (honeypots, …)
6. Network intrusion detection systems.
7. An independent ticketing and case management tool to manage incidents.
8. End-point security solutions (EDR, …)
9. Context and extended visibility (identity access management, PAM) and File Integrity Modules (FIM).
10. Other SOC-related technologies like UBEA (supervised, un-supervised), SOAR…

The civil work and SOC room fit-out are also required as part of the project.

3.3 Solution overview

Please describe using two to four pages your general methodology to implement a mature SOC. The narrative can include some recommended features/components that are not necessarily requested in Section 3.2 *and deemed essential in implementing your approach.*

"The bidder's methodology should:

- *Include their intent on how they cover the environment security; taking into consideration all cyber kill chain phases (Reconnaissance, Intrusion, Exploitation, Privilege escalation, Lateral movement, Obfuscation/Anti-forensics, Denial of service, Exfiltration)*
- *Highlight their tools and protection application taking in to consideration critical use cases, logging enhancement, customization, etc.*
- *Include a high-level design of their solution"*

4 Submission

Expressions of interest shall be submitted to ICMPD by October 7th, 2019 17:00 (Vienna Local time) to procurement@icmpd.org including the following documentation:

1. Registration Country
2. Power of attorney for the employee submitting the Expression of Interest.
3. List of products suggested for the project.
4. Probable country(ies) of origin for the products.
5. If there are any patents, kindly inform who has the right to fabricate these products.
6. List of Personnel occupying key positions in the company.
7. Team members who will be involved in this project.
8. Copy of passports of the above team members and owners of the company (or companies in case of a consortium).
9. Documents as requested for in Section 3.

Late submissions shall be disqualified

CALL FOR EXPRESSION OF INTEREST

Please reply to the subject Call for Expression of Interest and provide information about your company by completing the below table and attaching a current version of your company brochure or any relevant company information.

Company name:	
Business nature :	
Address :	
Contact person :	Position :
Telephone no :	Mobile no :
E-mail :	Company web site:

Completed and signed by: Name and position:

Date:

Disclaimer:

Calls for Expressions of Interest do not constitute a solicitation. ICMPD reserves the right to change or cancel the requirement at any time during the call for expression of interest and/or solicitation process.

Nothing in or relating to this Call for Expression of Interest shall be deemed a waiver, express or implied, of any of the privileges and immunities of ICMPD.

ICMPD reserves the right in selecting the invitees for the subsequent competitive bidding exercise based on substantial and proven records of performance in the subject field of activities. The mere expression of an interest would not automatically warrant for participation in such subsequent competitive bidding exercise.