Terms of Reference for Endpoint Security Renewal and Managed Services

Overview:

Maldives Ports Limited (MPL) is seeking a party to renew Endpoint Security licenses, deploy a SIEM solution, and provide managed services for Endpoint Security over a period of one year. The selected party will be responsible for actively monitoring the health and security of the endpoints and reporting any findings to the relevant MPL IT team.

General Requirement:

1. **Endpoint Security solution:**
    a. The solution must be either SentinelOne or CrowdStrike with the latest version.
    b. Licenses valid for 1 year.
    c. Total number of endpoints to be licensed: 700.
2. **SIEM solution:**
    a. Deploy a SIEM solution that seamlessly works with the Endpoint Security solution. Any dependencies must be detailed in the proposal.
    b. If the solution involves a third-party product, it must be integrated with the Endpoint Security solution.
    c. The SIEM solution should support configurable anomaly detection to identify potential security threats or unusual behavior in the systems and network traffic.
    d. The vendor must configure the anomaly detection based on our environment and provide configuration tuning.
3. **Managed Services:**
    a. Manage the overall security and health of the endpoints.
    b. The selected party must offer 24/7 round-the-clock technical support, including issue reporting and assistance, with escalation paths for critical incidents.
    c. The incident response partner should provide regular reports on threat hunting findings, detected threats, and incident response activities.
    d. Clear communication protocols for proactive alerts, incident updates, and ongoing security status updates must be established.
    e. Security analysts from the incident response partner should be available for direct communication and consultation on security concerns and/or incidents.
    f. The proposed solution must include service level agreements with guaranteed response times: within 1 hour for priority 1 incidents, within 2 hours for priority 2 incidents, and within 8 hours for priority 3 incidents. A categorization matrix for incidents and reporting structure must be included.
    g. Services must be provided for a duration of one year.

Eligibility Requirements:

1. **Experience in Cybersecurity, Digital Forensics and Incident Response:**
    a. The firm must possess at least five (5) years of verifiable experience in either conducting cybersecurity audits and implementation or handling incident response and digital forensics.
    b. The selected party must provide at least five references from prior incident response services delivered within the region, including details of the services provided.
    c. A letter of reference or contact information must be provided for verification.
2. **Incident Response Support:**
    a. The selected party must be an authorized incident response partner along with certified engineers for the proposed product, providing support during threat hunting campaigns, assisting with investigation, containment, and remediation of identified threats.
3. **Subcontracting:**
    a. The selected party is not permitted to subcontract any part of the project to a third party. All work must be performed by the selected party's own team.
4. **Local Engineers:**
    a. The selected party must have at least two locally based engineers/team members certified by the vendor, with their profiles or qualifications submitted for review.
5. **Police Reports:**
    a. The selected party must provide police reports for all team members who will be involved in the project, demonstrating that they have no criminal records.

Evaluation Criteria:

The proposals will be evaluated based on the following criteria:

Criteria	Marks
Quoted Price Lowest Price will be awarded full marks.	**60**
Educational Qualifications of the Proposed Team 5 points will be awarded for each cyber security related certification/credential awarded by a reputable body. (minimum 2 certification for a team member)	**20**
Experience of the Firm and its Proposed Team 4 points will be awarded for each valid reference indicating that the work, involving MSSP and/or incident response, was carried out by either the proposing firm or a team member.	**20**