TOR for a National Cyber Security Advisor

Introduction

- National Centre for Information Technology (NCIT) was established on the 25th of March 2003 by Government of Maldives as the main government agency for the development, promotion and propagation of Information Technology (IT) in the Maldives.
- Hence, to ensure the security of its systems and infrastructure, NCIT requires the services of a cybersecurity expert to act as an independent **National Cyber Security Advisor**.

The Scope of work

1. Proactive Cyber Threat Hunting on e-Government Infrastructure. The client must conduct regular tests for compliance with security policies and procedures to ensure security measures are protecting the organisation.
2. Analyse and assesses vulnerabilities in the infrastructure (software, hardware, networks), investigate available tools and countermeasures to remedy the detected vulnerabilities, and recommends solutions and best practices to protect against an attack from internal and external attacks.
3. May assist in the creation, implementation, and management of Security Solutions.
4. The retainer must prepare reports for the client, detailing the weak security areas and make recommendations to correct the problems.
5. Assist with the validation of the security posture of new changes to the Infrastructure of National Computer Network and e-Government Hosting Infrastructure and advice required changes.
6. Attend to incidents handling and response requested by Government and state organisations. Analyse and assess damage to the data/ Infrastructure as a result of security incidents, examine available recovery tools and processes, and recommends a solution.
7. During the incident handling and response, the advisor should submit forensic evidence to identify patient zero. Initiate the remediation process and propose recommendations to mitigate future threats. Discover indicators of compromise (IOCs) or create new IOCs from

incident handling and response processes for cyber threat intelligence, which can be used for mitigations across the government in future as a reference on attacker patterns.

8. Alert the organisation on new cyber threats to be published to the media.
9. Assist during the implementation process of the National Security Operations Center and the National Computer Emergency Response Team (CERT).

Deliverables

1) Conduct a security assessment of e-government applications per request.
2) Conduct a continuous assessment of eGovernment infrastructure and submit a monthly report to the management with recommendations to protect against cyber threats.
3) Conduct an internal vulnerability assessment and penetration testing of NCIT and the e-Government infrastructure within the first three months.
4) Proactive Cyber Threat Hunting on e-Government Infrastructure and provide all IOCs.

Experience/ Skills

- The candidate should have a minimum of 5-year experience in the field of cybersecurity. The candidate should submit references (such as reference letters or contacts and details).
- Have in-depth knowledge of attack and defence mechanisms.
- Should have a thorough knowledge in Windows and *nix Operating Systems
- Experienced in OS hardening.
- Networking and Virtualization environments security.
- SIEM designs for proactive threat hunting.
- Forensics and Anti-Forensics (Rootkits).
- Application Layer Vulnerability Assessment and Penetration Testing.
- WLAN Penetration Testing for 802.11 & 802.1x.
- Memory Forensics.
- Understanding of Database Administration or MS DBMS FCI and Availability Groups
- Knowledge in Enterprise SANs.
- Physical Security.
- Custom Scripting for Digital Forensics and Incident Response.
- Active Directory Security Implementations.

Education

- The candidate should submit internationally accepted certificates, that relates to ethical hacking, cybersecurity and digital forensics.

Core Competencies:

- **Ethics and Values:** Demonstrate and safeguard ethics and integrity;
- **Organisational Awareness:** Demonstrate corporate knowledge and sound judgment;
- **Development and Innovation:** Take charge of self-development and take initiative;
- **Work in teams:** Demonstrate ability to work in a team environment and to maintain effective working relations with people of different technical and non-technical backgrounds;
- **Communicating and Information Sharing:** Facilitate and encourage open communication and strive for effective communication;
- **Self-management and Emotional Intelligence:** Stay composed and positive even in difficult moments, handle tense situations with diplomacy and tact, and have a consistent behaviour towards others;
- **Conflict Management:** Surface conflicts and address them proactively acknowledging different feelings and views and directing energy towards a mutually acceptable solution;
- **Continuous Learning and Knowledge Sharing:** Encourage learning and sharing of knowledge;
- **Appropriate and Transparent Decision Making:** Demonstrate informed and transparent decision making.

Contract Duration

- The contract duration will be one year's renewal based on performance.

Monthly Remuneration Package

- Maldivian Rufiyaa (MVR) 25,000/- paid as a flat monthly fee upon submitting an invoice.

Application Deadline

- 19th August 2019
- 10:00
- Submit documents in a sealed envelope to:
    - National Centre for Information Technology
      No 64, Kalaafaanu Hingun,
      Male', Republic of Maldives.

Application Documents

- Interested candidates should submit:
    - Copy of National Identity Card

- The CV (Should contain a list of references with contact numbers)
- Copies of relevant certificates
- Reference letters proving the candidates are well versed in the cybersecurity field.

Marking Criteria

Experience and adequacy for the assignment	
Five years experience in the cybersecurity field	10 Marks
More than five years of experience in the cybersecurity field	20 Marks
2 Years of experience in managing data centre infrastructure	20 Marks
Academic Background	
Bachelors Degree in Business, IT, computer science or related field	5 Marks
Masters Degree in Business, IT, computer science or related field	10 Marks
Specialised Certificates in cybersecurity and IT related fields	35 MArks