Terms of Reference
Cybersecurity Consultant

Introduction

Election Commission of Maldives (herein referred as ECM) invites individuals to submit application for a Cybersecurity Consultant. ECM requires the service of a Maldivian Cybersecurity expert to act as an independent retainer-based Cybersecurity Consultant.

A) Scope of Work

1. Assisting in developing and implementation of strategies and best practices of cybersecurity; Ensuring the dissemination of best practices in the fight against existing and emerging cybercrimes.
2. Proactive Cyber Threat Hunting ECM's ICT Infrastructure. Must conduct regular tests for compliance with security policies and procedures to ensure security measures are protecting the organization.
3. Analyze and assess vulnerabilities in the infrastructure (software, hardware, networks), investigate available tools and counter measures to remedy the detected vulnerabilities, and recommend solutions and best practices to protect against internal and external attacks.
4. Assist in the creation, implementation, and management of Security Solutions.
5. The retainer must prepare reports for ECM, detailing the weak security areas and make recommendations to correct the problems.
6. Analyze and assess damage to data or Infrastructure of ECM 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 organization in future as a reference on attacker patterns.
8. Alert the supervisor on new cyber threats and recommend security measures to be taken.

B) Deliverables

1. Just-in-time technical assistance, delivered, as required
2. Overall Cyber Security Strategy and Work Plan
3. Human capacity development at ECM IT Team.
4. Proactive Cyber Threat Hunting on ECM ICT Infrastructure and provide all IOCs.

C) Experience/ Skills

1. Proven experience in cyber security tasks at high-level Government institutions and various other stakeholders with minimum of experience of 5 years in ICT security, Cyber Security Incident Handling and Response and digital forensics, in the public and private sector.
2. Demonstrated capabilities in consulting specialists, in fields such as technology, privacy, security, interconnection and etc.
3. Hands on experience in virtualization, DBMS, SAN, firewall and handling complex enterprise environments.
4. Have in-depth knowledge of attack and defense mechanisms.
5. Should have a thorough knowledge in Windows and Linux Operating Systems
6. Experienced in OS hardening.
7. Networking and Virtualization environments security.
8. SIEM designs for proactive threat hunting.
9. Forensics and Anti-Forensics (Rootkits).
10. Application Layer Vulnerability Assessment and Penetration Testing.
11. WLAN Penetration Testing for 802.11 & 802.1x.
12. Memory Forensics.
13. Understanding of Database Administration or MS DBMS FCI and Availability Groups
14. Knowledge in Enterprise SANs.
15. Custom Scripting for Digital Forensics and Incident Response.
16. Active Directory Security Implementations and security hardening.
17. Participation in internationally recognized specialized training for cybersecurity

D) Contract Duration

a. The contract duration will be up to the end of the work of Presidential Election 2023.

E) Monthly Remuneration Package

a. Maldivian Rufiyaa (MVR) 30,000/- paid as a flat monthly remuneration.

F) Application Documents

Interested candidates should submit:

a. Application Form
b. Copy of National Identity Card
c. The CV (Should contain a list of references with contact numbers)
d. Copies of relevant certificates
e. Reference letters proving the candidates are well versed in the cybersecurity field.

G) Qualification

1. Completion of MQA level 9 certificate in Cyber Security or in a related field, with professional work experience of minimum 1 year. OR

2. Completion of MQA level 7 or 8 certificate in Cyber Security or in a related field, with professional work experience of minimum 2 years. OR

3. Completion of MQA level 5 or 6 certificate in Cyber Security or in a related field, with professional work experience of minimum 3 years. OR

4. Over 5 Years' experience in leading a cyber security team in a government organization. OR

5. 2 years or more experience in advanced digital forensics in incident handling and response. OR

6. 2 or more years of experience in managing Datacenter infrastructure. OR

7. Specialized Certifications in cybersecurity and IT related fields with work experience of minimum 2 years

Disciplines: IT, Computer Science