ធនាគារ ស្ថាបនា
SATHAPANA BANK

Manager of IT Incident Handling and Forensic

Phnom Penh, Cambodia | Closing Date: 25th March 2019

Apply to Sok.Socheat@sathapana.com.kh

Job Description

The prime responsibility is to plan, manage, direct and coordinate the IT incident response and forensic to ensure effectiveness and efficiency in managing IT incident, and forensic operation.

Responsibilities

- Establish/enhance standard incident response plan to ensure the bank is able to react quickly in the event of an incident, determine a non-incident, operate efficiently during incident, and improve after an incident.
- Plan, coordinate and implement incident response exercise regularly based on designed scenario and report exercise result with lesson learn, and ensure the readiness of well managed incident response team can detect and react to incident effectively and timely.
- Establish and organize a forensics capability which be able to determine the root cause of incident and followed the standard investigation process or industry accepted forensic methodologies, and ensure forensic team are well trained and capable to perform inspection, in-depth analysis of suspected case and security breach.
- Investigate all identified security breaches, or concentrated attempts at breaching IS/IT policies, and arrange, coordinate third party investigator/consultant if required.
- Provides in-depth analysis of suspected malware, infected systems, network devices, and develop standard investigation report and ensure timeliness, completeness, and accuracy for related case reporting.
- Ensure daily monitoring and analyzing system log is performed to identify and block malicious behavior, activities, and provide analysis and trending of security log data from a large number of varied system and security devices.

Qualifications

- 4 to 7years' experience related to information/technology security, cyber security
- Knowledge of and experience with security regulations and standards including NIST, SANS, PCI, ISO/IEC, CIS
- Knowledge of TCP/IP Protocols, network analysis, and network/security applications
- Experience in Cyber incident response
- Experience on system log/event analysis, SIEM, IPS, IDS, Firewall
- Experience performing computer forensic with forensic tool/program
- Must be able to be adaptable, focused, accountable, and helpful
- Ability to work under pressure and meet deadlines
- Leadership and team work

How to apply

- Interested candidates are encouraged to submit the updated CVs and Cover Letters to job@sathapana.com.kh or Sok.Socheat@sathapana.com.kh
- For more information, please contact us via 096 958 7777/ 096 418 2222 or go to www.sathapana.com.kh