ធនាគារ ស្ថាបនា
SATHAPANA BANK

Senior IT Incident Handling & Forensic

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

Apply to Sok.Socheat@sathapana.com.kh

Job Description

The prime responsibility is to assist in managing, directing and coordinating the IT incident response and forensic to ensure effectiveness and efficiency in managing IT incident, and forensic operation.

Responsibilities

- Advise on information security issues and provide effective recommendations to mitigate the risk at acceptable level.
- 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.
- Ensure any related forensic manual(s) and procedure(s) are in place and regularly update.
- Investigate all identified security breaches, or concentrated attempts at breaching IS/IT policies, arrange and coordinate third party investigator/consultant if required.
- Provides in-depth analysis/investigation of suspected malware, infected systems, network devices, and develop standard investigation report and ensure timeliness, completeness, and accuracy for related case reporting.
- Continuously monitor, maintain and tuning security tool/systems used to identify, detect and properly respond to unknowns or alerts triggers.
- Reconcile threats from multiple data sources, setting event thresholds and updating signatures/sensitivity.
- Provide threat and vulnerability analysis as well as security recommendation
- Other duties as assigned.

Qualifications

- Bachelor Degree in Information Technology, Information Security, Cybersecurity, or related field.
- 2 to 3 years' experience related to information/technology security, cyber security, security operation center
- Knowledge 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 adaptable, focused, accountable, and helpful
- Good verbal and written in English.
- Good customer service skills

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