# Job Description

| | |
|---|---|
| Position: | **Officer, IT Security Analysis** |
| Department: | IT Security |
| Reporting to: | Supervisor, IT Security Analysis |
| Location: | Headquarter |

## I. Duties and Responsibilities

- Ensure the identification of required security related issues, and that they are alerted upon by configuring and establishing monitoring, correlation, and alerting solutions.
- Correlate all reported events from various multiple systems and network areas where potential security incident is identified; ensure the situation is handled promptly and effectively by starting the process of security incident response.
- Carry out configuration and maintenance of the implemented SIEM solution to enable it effectively to identify and alert upon potential security events, as well as reduce the false positives simultaneously.
- Work with major service providers or vendors to resolve security issues identified with their managed systems and infrastructure in line with the company's incident response requirements.
- Make recommendations for changes to the environment that can help in the removal of vulnerabilities and reduction in the risk of exploitation that may result in potential incidents.
- Identify potential weaknesses and implement measures, such as firewalls and encryption
- Liaise with stakeholders in relation to cyber security issues and provide future recommendations.
- Maintain an information security risk register and assist with internal and external audits relating to information security.
- Monitor and respond to "phishing" emails and "pharming" activity and guidance to staff on the issues such as spam and unwanted or malicious emails.
- Generate reports for both technical and non-technical staff and stakeholders.
- Lead and conduct the email phishing simulation exercise and related security simulation exercises.
- Perform other IT security tasks assigned by line manager.

## II. Qualification

- Bachelor's degree of IT, Computer Science, or another related field.
- 2+ years in Security Operations Center (SOC) experience.
- Working knowledge of anti-malware, vulnerability management, intrusion detection/ prevention systems, end point security and access management.
- Have a good understanding of networking and routing protocols, including TCP/IP.
- Proven experience in Unix / Linux system administration.
- Knowledge of IT Security auditing processes.
- Good in analytical skills.
- Good verbal and written English skills to present to senior management.
- Good negotiating, influencing and conflict management skills.
- Good verbal & written communication skills, as well as excellent listening and interpreting skills.
- Self-starter and with team leading experience.
- Attention to details and accuracy.