

## **Position : Cyber Security**

### **Job Responsibilities:**

- Oversee security of IT systems & infrastructure across the Organization and to ensure stability and availability of IT critical systems which have major impact on business continuity plan.
- Responsible for ongoing risk assessment for IT Infrastructure, System & Process and ensure compliance to regulatory standards, practices and guidelines, ex: ISMS (Information Security Management System)
- To report promptly any breach of law, regulation, the company's code of conduct or other company policies and guidelines to immediate superior.
- Establish and improve the processes for IT security management system.
- To administer and enforce IT Security Policies, Procedures, Standards and Process to all IT systems and network platform.
- Conduct operational and process reviews in compliance with all regulatory standards, ex: ISMS (Information Security Management System)
- Advise the effectiveness of corrective actions pertaining to any weaknesses in security audit findings.
- Assess / Respond / Investigate IT security vulnerabilities and risks. Additionally, to ensure corrective action plans are initiated and monitored.
- Evaluate, recommend and implement security tools and services to align security posture according to business need.
- Responsible for security & policy administration of nominated systems, ID management, program movement/version upgrade.
- Responsible for incident & problem analysis and ensure countermeasure is implemented to prevent reoccurrence.
- Will be responsible on Security Operations works, such as SOC.

### **Job Requirements:**

- Bachelor's Degree holder in Computer Science/Information Technology/Information System or equivalent.
- Minimum 5 years of IT security & risk exposure in service-provider, vendor or financial institution.
- Have a strong knowledge in networking, would be able to understand and elaborate OSI Layers fluently.
- Have a strong and proven knowledge in operating system, such as Open Source (Linux, FreeBSD), Windows and any traffic analysis software/tools, ex: Wireshark, TCPDUMP, TCPFLOW etc.
- Preferably with CISSP, CISM, CEH or any other professional certification of IT/IS Security.
- Familiar with standards and requirements such as ISO27001, PCIDSS and any financial authorities (RMIT-Bank Negara) will be an added advantage.
- Broad knowledge of IT Security and control solutions including Firewall, VPN, Security Incident Event Management (SIEM), Intrusion Detection System (IDS), Anti-Virus, Compliance Monitoring Tools, Data Leakage Protection (DLP), Web Application Firewall (WAF), Web Proxy Gateway & File Integrity Management (FIM), ANTI DDOS Solutions.
- Familiar with the Blue & Red Team Operations.



- Have a good understanding on ATT@CK Mitre Framework.
- Able to demonstrate company values of integrity, collaborative, professionalism, customer centricity, forward thinking and mindfulness at all time.
- Applicants must be willing to work in Cyberjaya, Selangor.

