Job Title : IT Security Analysist / Penetration Officer

OVERALL PURPOSE:

- IT Security Analyst is responsible for preventing data breaches and securing computer and information systems. S/he is also responsible to develop, implement, and maintain the Bank secure posture following information security policy, standards, guidelines, and procedures to ensure that all information systems are functional and secure.

RESPONSIBILITIES:

Main Responsibilities

- Develop, implement, and maintain information security policy, procedures, and standards
- Conduct security monitoring on the Bank computer networks to identify cybersecurity issues
- Conduct digital forensic and investigate on security breaches or other cybersecurity incidents
- Document security incidents, provide recommend remediation, and develop mitigation plans to prevent future cybersecurity incident
- Initiate security programs to enhance security layers on the operating system, network devices, and so on
- Initiate and coordinate on patch management and deployment schedule
- Simulate internal phishing activity to measure end-user awareness
- Implement and manage security tools such as Web Application Firewall (WAF), Endpoint Detection and Response (EDR), Security Information and Event Management (SIEM), and Privilege Access Management (PAM)
- Conduct information security risk assessment program and simulate security use-cases to improve security detection system
- Prepares the disaster recovery plan (DR/BCP) and assist in coordinating contingency plan tests on a regular basis
- Initiate and conduct cybersecurity awareness program for staffs across the bank
- Stay up-to-date on cybersecurity trends and zero-day vulnerabilities

Others:

- Respond to enquiries from staff and provide security advice as required;
- Work with technology related team/department to make smoothly operation of the Bank businesses, and ensure IT operation functions meets business requirement;
- Willing to learn new things and got global cyber certified;
- Other job assigned.

QUALIFICATIONS REQUIREMENTS:

- Bachelor in of Information Technology, Information Security, Cyber Security, or other related degrees such as Computer Science, Management of Information Systems;
- At least 1-3 years working experience in IT security, IT governance or other IT security Related;
- Holding security related certification in CySA+, ECSA, OSCP, CEH, CISA or from equivalent recognized certification body is a plus;
- Broad knowledge of a wide range of Information Technology and Digital systems and a deep understanding of the inherent security risks associated with these technologies;
- Possess good knowledge of cyber security standards or frameworks such as TRMG, NIST, CIS or ISO27001;
- Understanding of IT Security solution/tools (SIEM, PAM, Antivirus, Vulnerability Scanning, and IDS/IPS);
- Experience with penetration testing and vulnerability assessment project;
- Proven ability to identify, mitigate vulnerabilities, and provide easy to understand reports, deliver presentations on information risk management, systems process control;
- Positive attitude towards learning and development demonstrated by a record of continuing professional development;
- Self-confident and able to work under pressure;
- Good working knowledge of information risk analysis/management;
- Ability to manage time and priorities appropriately;
- Good verbal and written communication skills and able to communicate effectively at all levels;
- Honesty, reliability, and a commitment to strict confidentiality.

Contact Info:
Email: hr@vattanacbank.com
Phone Number: 023 963 999 / 070 723 747