1. JOB TITLE: Specialist: Cyber Threat Hunting - Forensic Analysis

Line Manager- Manager; Cyber Threat Hunting

Department- Cybersecurity

Location- HQ

Job Summary

Responsible for protection of system boundaries, keeping computer systems and network devices hardened against attacks and securing highly sensitive data. This includes analyzing digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

Key responsibilities:

- Implement and enforce Cyber security Policies to ensure alignment with related corporate policies.
- Understand and provide expert advice on the Cyber security risks facing information assets.
- Responsible for the technical Cyber security strategy – proposing and implementing solutions and processes to continuously reduce the risks and effects of hacking and cyber-crime.
- Responsible for forensic investigation of Cyber security incidents/breaches, providing regular reporting using the appropriate assurance framework.
- To coordinate regular security testing with high quality reporting. Responsible for the subsequent hardening of IT systems based on results of regular tests.
- Develop custom scripts or tools to automate the analysis and handling of unique or complex digital forensic challenges.
- Conduct analysis of log files, evidence, and other information to determine the best methods for identifying the perpetrator(s) of a network intrusion.
- Provide technical summary of findings in accordance with established reporting procedures.

- Run various assessment tools to obtain insight on security posture and create various reports for management and stakeholders.
- Utilize specialized software tools to identify and investigate digital footprints and artifacts left by cybercriminal activities.
- Collect and analyze intrusion artifacts (e.g., source code, malware, and system configuration) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise.
- Monitoring of all IT assets on configuration integrity in order to proactive manage the bank's environment.
- Identify and define system security requirements standards of the bank.
- Responsible for regular security testing with high quality reporting. Responsible for the subsequent hardening of IT systems based on results of regular tests.
- Support penetration testing activities and exercises, including self-capacity to perform penetration testing.
- Recommend assessment-based findings, outcomes, and propositions for further system security hardening enhancement.
- Analyze file systems, including FAT, NTFS, and EXT, to recover deleted files and hidden data.
- Responsible for information security awareness and training program that informs and motivates workers on cyber-security matters as per the SAT program.
- Monitor internal and external policy compliance and cybersecurity framework is being complied by both vendors and employees.
- Use a range of forensic tools and software to extract and analyze data.
- Implement new technology on the network security and ensure security hardening and effectiveness of the control. Implement and Ensure compliance of Cybersecurity framework amongst the organization.
- Participate in the incident response program, ensuring that the program is tested throughout the organization and that every staff knows his or her duties during such an incident.
- Prepare and report all security incidents and Forensic investigation to Management or as directed by line manager.
- Conduct research on emerging technologies and their implications for digital forensic investigations, including blockchain and IoT devices.

Experience, Knowledge and Skills Requirements

- Bachelor Degree in Computer systems technology or related academic field.
- Minimum of 3 years of ICT Security experience in banking environment, Expert knowledge of current IT cyber security issues.
- At least 1 ICT Security professional certifications, CISA, CISSP, CEH, CISM, CFCE etc.
- Knowledge of security Issues and products so that complex security issues can be quickly diagnosed and resolved.
- Report writing and procedure /policy development.
- Management of a complex IT Infrastructure within large enterprise level organization.
- Contingency and Disaster Recovery Planning.
- Ability to think ahead and anticipate problems, issues, and solutions.
- Experience providing IT focused Enterprise Architecture and strategy.
- Windows Operating systems and Active Directory Management.
- Anti-Virus domain infrastructure.

Deadline: 21st April 2024

APPLY HERE

2. JOB TITLE: Specialist; Security Operations Center (SOC)- 2 Positions

Line Manager- Manager; SOC

Department- Cybersecurity

Location- HQ

Job Summary

Support in ensuring that the Bank's information is protected in accordance with the needs of the business and according to Information Security principles of availability, integrity and confidentiality. To bring the organization's information security risks under explicit management control through implementation of controls and close monitoring. To support the technical implementation of the Security Incident and Event Management (SIEM) toolset.

Key responsibilities:

- Responsible for building relationships with teams across the company to understand current and future security threats and vulnerabilities at the direction of the SOC Manager.
- Steer work on the design and operation of current and future toolsets that will support the SOC development, as per current understanding of future scenarios; namely alerting, monitoring, and reporting.
- Accountable for the development of long and short technical capabilities, including software and hardware requirements; gathering business requirements; developing initial findings and working to agree a prioritised list of technical capabilities and projects with the assistance of the SOC Analyst.
- Support SOC development roadmap by delivering SOC capabilities to the business and championing new ideas and initiatives to help improve new and existing capabilities
- Responsible for ensuring that SOC delivery for Information Security is aligned with Information security policy, related information security standards and guidelines.
- Deliver Information Security related support across a wide range of technology issues to technology and business leaders and their teams across various departments within the business.

- Make recommendations to various project teams and sponsors across the business regarding Security Monitoring requirements and log data feeds that will need to feed into the SOC when new business functions are conceived to ensure all the Information Security requirements are captured at the earliest opportunity.
- Responsible for ensuring all relevant technical standards and policy documentations are reviewed and maintained thought-out each of the SOC technical capabilities
- Responsible for integration of standard and non-standard logs in SIEM and central log management solutions.
- Responsible for ensuring that relevant request forms for each of the SOC capabilities have been completed correctly, assessed, and actioned in a timely manner.
- Manage technical relationships with key personnel to ensure that all work is aligned to help deal with any issues or problems and the same are followed up and dealt with appropriately.
- Represent the Information Security team at internal and external meetings and forums as agreed by the SOC Manager.
- Required to communicate and collaborates at all technical levels throughout the corporation, and with external parties including liaise with and manage outsourced service providers.
- Perform scheduled and ad-hoc security assessments across the Bank systems and networks, ethically, to identify loopholes and devise remediation actions, acting as part of red team and assisting the cyber security blue team in resolution of identified flaws. Security assessments include but not limited to penetration testing, cracking and ethical hacking.

Experience, Knowledge and Skills Requirements

- Bachelor's degree in computer systems technology or related academic field.
- Minimum of 3 years' experience in Cyber security operations.
- At least 1 ICT Security professional certifications, CISA, CISSP, CEH, CISM, CFCE etc.
- Experience in implementing and managing SIEM solutions.
- Experience of working in a deadline-oriented incident management environment managing multiple issues simultaneously.
- Technical handling interaction with vendors, contractors, and other stakeholders
- Experience in operating big data forensic technologies.
- Experience in operating VMware implementations.
- Understanding of ISMS concepts.

Deadline: 21st April 2024

APPLY HERE

3. JOB TITLE: Product & Service Design Manager- 2 Years Contract

Line Manager- Head; Business Transformation

Department- Business Transformation

Location- HQ

Job Summary

Responsible for leading and managing the products and services innovation lifecycle from ideation to launch. The role requires a deep understanding of market trends, customer needs, and the competitive landscape to develop and introduce breakthrough banking products that deliver value to customers and differentiate the bank in the market.

The job holder shall act as an expert by being a trusted “go to person” for guiding product owners an key stakeholders on implementation of the PLM practices, to ensure the Bank achieves its strategic results.

Key responsibilities:

- Lead the product development team to identify, develop, and manage new product ideas that align with the bank's strategic objectives.
- Conduct market research and competitive analysis to identify product and service innovation opportunities.
- Collaborate with cross-functional teams, including technology, marketing, finance, and operations, to implement product and service strategies.
- Foster an innovative culture within the product team, encouraging creative thinking and risk-taking.
- Oversee the solution design process to ensure products and services meet customer needs, policy requirements, and regulatory standards.
- Document business cases for new products, including financial modelling, risk assessment, and market entry strategies.
- Manage the product development pipeline, ensuring timely progression of products from conception to market launch.
- Establish metrics to measure the performance of products and services to promote continuous improvement.
- Keep abreast of emerging technologies and fintech trends to ensure the bank remains at the forefront of product innovation.
- Manage relationships with research firms, data providers, and innovation partners, ensuring quality services and cost-effective agreements.

Experience, Knowledge and Skills Requirements

- Bachelor’s Degree in business, Finance, Economics, Marketing, or a related field.
- Proven experience of minimum 5 years in solution development or product management within the services industry.
- A strong track record of successfully developing and launching innovative products.

- Knowledge of regulatory requirements related to product governance and market intelligence.
- Strong interpersonal skills with the ability to build and maintain relationships with internal and external stakeholders.
- Demonstrated ability to work independently and collaboratively in a fast-paced, dynamic environment.
- Solid understanding of banking products and services, along with digital banking trends.
- Excellent leadership and people management skills.
- Strong analytical and critical thinking abilities and creative mindset willing to challenge the status quo.
- Exceptional project management skills.
- Effective collaborator with the ability to work in a cross-functional environment.

Deadline: 17th April 2024

APPLY HERE