Job Title	Principal Engineer, Cyber Security Operations	**Reports To:**	Head of Technology Security
Division:	Digital Business	**Department:**	Technology - Engineering
Grade	Band 5	**Date:**	May 2024

JOB PURPOSE STATEMENT

The Principal Engineer, Cyber Security Operations will be responsible for day-to-day running of security programs such as Patch and Vulnerability Management, Incident Response and Security Monitoring. The role will work with NCBA Group Cyber team to manage support SLAs. They will also be responsible for managing and closure of Technology audit issues in Digital Business and maintaining an up to date asset register.

The role will lead and coordinate all cyber security operation activities in 5 markets (Kenya, Tanzania, Rwanda, Ghana and Ivory Coast) in collaboration with NCBA group Cyber team.

KEY RESPONSIBILITIES & PERCENTAGE (%) TIME SPENT

- **Patch and Vulnerability Management:** Maintain a robust PVMG process by working with system and application custodians to ensure Vulnerabilities are closed within SLA. (25%)
- **Audit:** Track all audit issues within Technology and ensure they are closed within the agreed timelines. (35%)
- **Security Monitoring:** Onboard all Digital Business assets to SIEM and perform SOC L2 role for NCBA Digital Business systems. (25%)
- **Leadership:** Manage and coordinate cyber operation initiatives and ensure support SLAs are compliant. Define and report on key cyber operations metrics to senior management to measure return of investment in Cyber and Cyber risk management. (15%)

MAIN ACTIVITIES

- Perform regular Vulnerability assessment and Compliance hardening reviews on all NCBA Digital Business assets.
- Serve as the primary point of contact & escalation point for Security Administration tasks.
- Onboard all Digital Business systems to SIEM for monitoring by L1 teams.
- Perform SOC L2 role and investigate, close and report all cyber incidents affecting Digital Business Systems.
- Coordinate and track closure of all audit issues within Technology.
- Maintain an updated asset register for all servers and applications.
- Do regular follow ups with system custodians to ensure identified risks are addressed within the agreed timelines.
- Continuously review and improve cyber processes to ensure efficient support to the agile process of software development.
- Work with group Cyber to ensure that controls are well fine-tuned to protect NCBA Digital assets.

Decision Making Authority /Mandates/Constraints: What decision/s is the position holder empowered to make based on the key result areas of the position?
• Technical Decisions for security monitoring tools.

Planning: What planning responsibilities are applicable to this role? Indicate what the planning entails	
Type of Planning	**Duration of Planning**
Long Term Planning	One year
Short Term Planning	Quarterly and Annually for Performance Plans

Financial Responsibility: What financial responsibilities are applicable to the role? Indicate the amounts responsible for? The responsibility can be for OPEX, CAPEX, and Petty cash etc. Indicate what the financial responsibility entails e.g. approving, monitoring, reporting
N/A

Responsibility for stocks, equipment etc (non – cash resources). Indicate the type of resources responsible for and the approximate value.	
Resources, equipment, stocks etc.	**Approximate value (Kshs)**
N/A	

Responsibility for generating revenue. Indicate the revenue streams the position holder is responsible for as a % of the departmental target.
None

Relationship Management: The departments/organizations/companies etc that the position holder will need to relate/liaise with as part of this role
All business units

Project Management	
Type of projects	**Nature of responsibility**
Cyber security tools	Supplier

Process Management	
Type of Processes	**Nature of Responsibility**
Patch and Vulnerability Management Incident Response Change Management	Responsible Responsible Approver

COMPETENCE REQUIREMENTS

Excellent Interpersonal Skills

- The candidate relates easily and naturally with executives, business managers, technical teams and customers. Has excellent listening skills and understands the desires and challenges of all our leaders and customers.
- Candidate forms trusted relationships with technical teams and customers

Commercial Acumen

- The ideal candidate has broad knowledge of business and has an interest in market trends.
- With this knowledge, the candidate has researched and possessed an intricate knowledge of our business: its vision, mission, strategy, values and how it operates. They easily see how our business model compares with *trending local & world-wide* consumer demands.

Leadership & Communication Skills

- The ideal candidate can clearly communicate and share the planned cyber initiatives, reports, and risks with executives, business leaders, and stakeholders across the organization - in a manner that leaves them all touched, moved and inspired.

Innovative & Adaptable

- The ideal candidate is passionate about innovation.
- Loves technology and possesses both a deep and broad understanding of the technology market and cutting-edge technology and Cyber trends.
- Continuously listening to our stakeholder's feedback and coming up with new architectures and enhancing existing ones to leverage these *cutting-edge technologies*.

Self-Driven & Results Oriented

- Self-motivated and self-managing.
- Their work has had a material impact in attracting new customers, delighting existing customers, increasing our market share and enhancing our organizations efficiency and profits.
- Delivery model is organized around delighting our customers, increasing our profitability, and increasing the businesses efficiency.

Others

- Knowledge and experience in modern practices for Cyber security, Application Development and Agile Project management in medium to large Financial Institutions.
- Technical skills to effectively perform security testing activities/tasks across various technologies in a manner that consistently produce high quality of results.
- Knowledge and effective application of all relevant banking policies, processes, procedures and guidelines to consistently achieve required compliance standards or benchmarks.
- Self-empowerment to enable development of open communication, teamwork and trust that are needed to support performance and customer-service oriented culture.

QUALIFICATION AND EXPERIENCE REQUIREMENTS

- A Bachelor's degree in Computer Science, Information Technology or related field.
- Minimum of 5 years in Cyber Security systems administration e.g. Intrusion Prevention Systems, Web Application Firewalls, Remote access, Content Filters, endpoint protection, vulnerability management solutions etc.
- Information security certifications e.g. CEH/CISSP/CISM/CISA/GIAC/CPTP/OSCP
- Minimum of 2 years' working experience in Networking and Operating Systems e.g. Cisco, Huawei, Windows (All) and Linux.
- Hands on experience in software development with major languages Java, C++, C# and practical experience using relation RDBMS e.g. Oracle and MS SQL etc.
- Working knowledge of Cloud technologies in at least one of the following: AWS, Azure, Google and Huawei.
- Excellent analytical, problem solving and reporting skills
- A good knowledge of the systems and processes within Financial Services industry.
- Experience in leading teams of security analysts will be an added advantage.