Job Title:	Security Operations Centre (SOC) Analyst	**Reports to:**	Manager, SOC
Department/ Sub-department:	Information Security, Information Technology	**Division:**	Technology & Operations
Grade:	Band 2	**Date:**	
Job holder:		**Supervisor:**	
Signature:		**Signature:**	

Job Purpose Statement
The Cyber SOC (Security Operations Center) Analyst is responsible for monitoring and defending the organization's IT infrastructure against cyber threats. This role involves identifying, analysing, and responding to security incidents and vulnerabilities. The SOC Analyst plays a key role in maintaining the security of networks, systems, and applications, ensuring the organization's assets are protected from cyberattacks.

Key Results Areas

Perspective	**% Weighting** *(to add up to 100%)*	**Output**
SOC monitoring & Log management	60%	• Collect, review, and analyse logs from various security tools and infrastructure devices (e.g., firewalls, routers, servers) to detect anomalies. • Together with SOC MSSP This role shall manage security incidents through all phases of the incident response process through to closure. • Send weekly tools coverage for SIEM, DAM, Vulnerability management and the EDR
Information Security Processes	20%	• Ensure proper and conclusive resolution of reported issues • This role shall manage security incidents through all phases of the incident response process through to closure.
Audit and Risk	20%	• Support all Audit and Risk initiatives and assessments around SOC

Job Dimensions

Reporting Relationships: jobs that report to this position directly and indirectly	
Direct Reports	None
Indirect Reports	None

Stakeholder Management: key stakeholders that the position holder will need to liaise/work with to be successful in this role.	
Internal IT Department Enterprise & Compliance Risk Department Internal Audit	**External** External Auditors Regulators

Decision Making Authority /Mandates/Constraints: the decisions the position holder is empowered to make *(Indicate if it is Operational, Managerial or Strategic)*.
Operational –procedures and policy maintenance and implementation, audit management and planning

Work cycle and impact: time horizon and nature of impact (Planning) *(e.g. Less than 1 week, 2 weeks, 2 weeks – 1 month, 1month – 3 months, 3-6 months, 6-12 months, above 1 year)*
6-12 months

Ideal Person Specifications
• A Bachelor's degree in Computer Science, Information Technology or related field. • Minimum 3 years working experience in a busy IT environment. • Certification in a systems security or audit related area, such as CEH, CISA, CISM or CISSP. • Have a deep interest in computing and cybersecurity • Excellent analytical, planning and organizing skills • Familiar with methods for ethical security hacking/penetration testing • Knowledge of SIEM toolsets • Experience / Knowledge on security Incident Detection and Response • Familiar with the tools and techniques used by hackers • Excellent written and oral communication skills

Technical Competencies	
	• Bachelor’s degree in Cybersecurity, Information Technology, Computer Science, or a related field. • 1-3 years of experience in a Security Operations Center or a similar cybersecurity role. • Strong understanding of networking concepts (TCP/IP, DNS, HTTP, etc.) and network security protocols. • Experience with security tools such as SIEM (Splunk, ArcSight), EDR, firewalls, and IDS/IPS. • Familiarity with security frameworks such as NIST, ISO 27001, and MITRE ATT&CK. • Experience in incident response, log analysis, and vulnerability management. • Knowledge of malware analysis and threat hunting techniques is a plus. • Relevant certifications such as CompTIA Security+, CEH (Certified Ethical Hacker), or CISSP (Certified Information Systems Security Professional) are highly desirable.

Behavioural Competencies	
	• Strong analytical and problem-solving skills with attention to detail. • Ability to work well under pressure, particularly in incident response situations. • Good verbal and written communication skills, capable of reporting complex issues to technical and non-technical audiences. • Team player with the ability to collaborate effectively across different departments. • Strong understanding of confidentiality and ethical standards in handling sensitive information. • Self-motivated with a proactive attitude toward learning new skills and keeping up with industry trends.

This JD is signed-off with reference having been made to the organisation’s core values and aligned competencies against these values.