Information Security Analyst.

About us...
Cellulant was founded by Ken Njoroge and Bolaji Akinboro in 2002 with its business model initially designed on a napkin. Since 2002, the Cellulant team has learnt, adapted and leveraged their experiences to pivot the business to become the leading payments provider in the Continent. We have 400 staff, are physically present in 18 countries and provide services in 33 (countries).

Our purpose; Create opportunities that accelerate economic growth for all of Africa
Our mission; Enable seamless payments for businesses, banks and consumers across Africa

Our evolution over the years, from a digital content business, to mobile banking and now to payments has allowed us to build strong relationships and partnerships. We`ve taken our years of experience and assets acquired over the years to provide a payments platform in the continent that focuses on driving merchant business and digital payments for local, regional and global merchants in the Continent, and digitising both online and offline payments.

You can read more about us and our Group leaders and Country Champions by making use of the embedded links on this profile.

Responsibilities.

- Monitor and analyze Security Information and Event Management (SIEM) alerts to identify security issues for remediation and investigate events and incidents.
- Prepare reports that take note of security breaches and the extent of the damage caused by breaches.
- Monitor threat intelligence feeds.
- Respond to cyber security tickets and maintain the service desk queue for information security.
- Maintain cryptographic keys.
- Investigate, document, and report on information security issues and emerging trends.
- Access control management including weekly reviews.
- Installing endpoint security software and ensuring it is up-to-date and effective.
- Develop a security plan for best standards and practices for cloud computing, kubernetes and containerized environments
- Knowledge sharing with other teams.

Requirements
The preferred candidate will have Security Operations Center (SOC) and Incident Response/Coordination experience.

- Bachelor's Degree Computer Science, Cybersecurity, Information Security or equivalent.

- Experience with Security Operations Center, network event analysis and/or threat analysis.
- Deep understanding of Splunk Enterprise Security (will be an added advantage).
- Experience working as an Incident Responder/Coordinator.
- Deep understanding of Incident Response coordination when analysis confirms actionable incident.
- Able to fix complications with SSL, SSH, and SIEM systems and software.
- Deep understanding of various security methodologies and technical security solutions.
- Experience analyzing security logs from SIEM, Firewalls, Vulnerability Scanners.
- Experience monitoring threat feed sources.
- Experience with Endpoint Detection Response tools.
- Experience authoring Incident Response Playbooks.
- Experience and certification in digital forensics, an added advantage.
- Effective verbal and technical writing