Information Security Engineer.

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.
- Conduct continual vulnerability assessments and simulating offensive security testing
- Develop and review actions plans to remediate identified vulnerabilities and emerging threats against company information assets
- Endpoint security hardening
- Patch management
- Web and mobile app security testing and hardening
- Social engineering testing
- Threat hunting
- Information security awareness
- Continual technical risk assessment
- Weekly reporting

Requirements
- Bachelor of Science in Computer Science or a related field
- Five or more years' work experience as a System Security Engineer or related position
- Fluency in Linux, UNIX, Java, PHP
- Proven experience developing, operating and maintaining security systems
- Extensive knowledge of operating system and database security
- Knowledge of AWS container security

- Proficiency in networking technologies, network security and network monitoring solutions
- Knowledge of security systems including anti-virus applications, content filtering, firewalls, authentication systems and intrusion detection and notification systems
- In-depth knowledge of security protocols and principles
- Critical thinking skills and ability to solve complex problems.