Job Ref. No: JLIL 369

Position: Security Analyst

Jubilee Insurance was established in August 1937, as the first locally incorporated Insurance Company based in Mombasa. Jubilee Insurance has spread its sphere of influence throughout the region to become the largest Composite insurer in East Africa, handling Life, Pensions, Asset Management and Medical Insurance. Today, Jubilee is the number one insurer in East Africa with over 1.9 million clients. Jubilee Insurance has a network of offices in Kenya, Uganda, Tanzania, Burundi. It is the only ISO certified insurance group listed on the three East Africa stock exchanges – The Nairobi Securities Exchange (NSE), Dar es Salaam Stock Exchange and Uganda Securities Exchange. Its regional offices are highly rated on leadership, quality and risk management and have been awarded an AA- in Kenya and Uganda, and an A+ in Tanzania. For more information, visit www.JubileeInsurance.com.

We currently have an exciting career opportunity for a **Security Analyst** within **Jubilee Life Insurance Limited.** The position holder will report to the **Manager – IT Security** and will be based at our Head Office in Nairobi.

Role Purpose

The Security Analyst will be responsible for identifying, analysing, and mitigating security threats and vulnerabilities across the organisation's operational environments. The role focuses on proactive security testing, threat simulation, and vulnerability assessments to strengthen the organisation's cyber resilience, support regulatory compliance, and enhance the overall security posture of the organisation.

Key Responsibilities

Strategy

1. Support the development and implementation of security strategies and protocols to protect systems, networks, and data.
2. Collaborate with internal stakeholders to assess security risks and recommend preventive and corrective controls.
3. Continuously monitor emerging cyber security threats, technologies, and best practices to enhance organisational readiness.

Operational

1. Conduct penetration testing across internet, intranet, wireless, web applications, social engineering, and physical environments.
2. Execute red team exercises to identify gaps in security controls and incident response readiness.
3. Identify, analyse, and exploit security vulnerabilities across diverse systems and environments.
4. Lead or support penetration testing engagements, including providing technical guidance to junior team members.

5. Analyse test results and prepare clear, comprehensive reports outlining findings, risks, and remediation recommendations.
6. Communicate complex security concepts and findings to technical and non-technical stakeholders, including senior leadership.

Corporate Governance

1. Ensure compliance with regulatory requirements, industry standards, and internal information security policies.
2. Develop and maintain security documentation, including policies, procedures, and incident response plans.
3. Provide guidance to internal teams on security-related matters and support audit and compliance activities.

People and Culture

1. Promote a strong culture of security awareness and shared responsibility across the organisation.
2. Support knowledge sharing and skills development within the Cyber Security team.
3. Collaborate respectfully and effectively with cross-functional teams to embed security into everyday operations.
4. Model professional conduct, accountability, and ethical behaviour in all security engagements.

Key Competencies

1. Strong knowledge of penetration testing and vulnerability assessment techniques.
2. Ability to analyse complex security risks and recommend effective controls.
3. Strong interpersonal and communication skills.
4. High attention to detail and investigative mindset.
5. Ability to work independently and collaboratively within technical teams.

Key Deliverables for the Role

1. Conduct threat and vulnerability assessments with actionable remediation recommendations.
2. Investigate, document, and report information security incidents and emerging risks.
3. Analyse and respond to newly identified hardware and software vulnerabilities.

Academic Qualifications

1. Bachelor's degree in Computer Science or a related discipline from a recognised institution.
2. Information Security certifications such as CEH, OSCP, CompTIA PenTest+, or CRTP.
3. Networking certifications such as MCSE, CCNA, or CCNP.
4. IT Service Management certification (ITIL).
5. Cloud technology competency.

Relevant Experience

1. Minimum of 3 years' experience in penetration testing and vulnerability assessments.
2. At least 1 year of experience within a medium to large-sized organisation.
3. Hands-on experience with security testing tools, secure infrastructure reviews, and modern security technologies.

If you are qualified and seeking an exciting new challenge, please apply via Recruitment@jubileekenya.com quoting the Job Reference Number and Position by 31st December 2025

Only shortlisted candidates will be contacted.