

SECURITY OPERATIONS CENTRE (SOC) ANALYST - SOC/10/2026

REPORTING TO: HEAD OF INFORMATION SECURITY

Job Purpose: The SOC Analyst is responsible for continuous 24x7 monitoring, detection, analysis, and response to cybersecurity events across the Bank's technology environment. The role safeguards the confidentiality, integrity, and availability of systems, data, and digital services through intelligence-led monitoring, incident investigation, proactive threat hunting, and disciplined incident response, ensuring timely threat containment, regulatory compliance, and the uninterrupted delivery of customer-facing services.

Key Responsibilities:

- Monitor security alerts across security tools such as SIEM, EDR/XDR, NDR, IDS/IPS, WAF, DLP, email and cloud security platforms.
- Triage, analyse, and classify security events based on severity and impact.
- Investigate suspicious activity and escalate incidents in line with the Incident Response Plan.
- Tune detection rules, correlation logic, and thresholds to reduce false positives.
- Update detection logic with relevant threat-intelligence indicators.
- Identify automation opportunities and support SOAR playbook improvements.
- Support detection, containment, eradication, and recovery activities for security incidents.
- Preserve digital evidence in line with forensic and chain-of-custody standards.
- Tune detection rules, correlation logic, and thresholds to reduce false positives.
- Identify automation opportunities and support SOAR playbook improvements.
- Review threat-intelligence feeds relevant to the banking sector.
- Assess applicability of global threat alerts to the Bank's environment.
- Contribute to SOC KPIs and KRIs aligned to operational performance metrics.

Qualifications & Experience:

- Bachelor's degree in IT, Computer Science, Cybersecurity, or related field.

Professional Certifications (At least one preferred)

- Certified Ethical Hacker (CEH)
- Computer Hacking Forensic Investigator (CHFI)
- CompTIA Security+
- CISA/CISM
- ISO 27001 Foundation
- Any other relevant Cybersecurity certification

Key Competencies:

- 1–3 years in SOC or cybersecurity operations (covers L1–L2 levels).
- Experience with SIEM, EDR/XDR, network security, firewall and endpoint logs.
- Experience in banking or regulated environments is an advantage.

ALL applicants **MUST** apply online to email: recruitment@familybank.co.ke; closing date is **03rd November 2026**. Canvassing will automatically disqualify the candidate. Only shortlisted candidates will be contacted.

"We are an equal opportunity employer"