CAREER OPPORTUNITIES

Applications are invited from interested and qualified persons for the following vacancies in The Kenya Power & Lighting Company PLC.

1. PRINCIPAL SECURITY ANALYST (1 Post)

Job Ref: HR: KP1/5B.2/1/3/1225

Reporting to the Manager, Security &Business Continuity, the Principal Security Analyst, will be responsible for the continuous monitoring of technology assets for security Incidents that impact on confidentiality, integrity and availability of systems across the Company. Overall security monitoring and incident response program of KPLC, including implementation of policies and procedures on security monitoring and incident response, by putting in place the appropriate people, processes and technology. Containment and recovery from security incidents or breaches.

The key tasks & duties for the position include;

- Primarily responsible for leading and managing a SOC team, and ensuring that security incidents are correctly identified, analyzed, defended, investigated, and reported.
- Monitor and analyze activity on networks, servers, endpoints, databases, applications, websites, and other systems, looking for anomalous activity that could be indicative of a security incident or compromise.
- Perform threat management & threat modelling, identify threat vectors and develop use cases for security monitoring.
- Ensure continuous integration of logs from technology assets into the SIEM to meet the security use cases.
- Manage the cyber incident response plan.
- Respond to incidents in accordance with the incident response plan.
- Effective communication and escalation during incident response.
- Focal point of contact for cyber incidents.
- Continuous improvement of the response plan.
- Develop and maintain the required Information Security policies, procedures and standard operating procedures (SOPs) in relation to the SOC and incident response, to strengthen the current Security Operations.
- Develop regular metrics, dashboards and reports for SOC operations for various stakeholders (IT Leadership, Senior Management.
- Develop SOC performance management tools.
- Ensure compliance to SLA and process adherence to achieve operational objectives.
- Leadership, mentorship and performance management for direct reports.
- Work closely and maintain a positive working relationship with internal teams and outsourced partners in the remediation actions of incidents within SLA.
- Direct and supervise the work of personnel and/or contractors assigned to the department.

Job Specifications:

- Bachelor's Degree in, Information Systems, Computer Science, Information Security or related field required.
- Seven (7) years' Technical Experience in a busy IT Environment with good understanding of all fields of IT and an appreciation for emerging technologies.
- Relevant certifications in Information Security knowledge areas, such as security monitoring, threat intelligence, Information Security Management and Ethical Hacking.
- Experience in security device management, and in SIEM, IPS/IDS, DLP, Active Directory and other security technologies.
- In-depth familiarity with security policies based on industry standards and best practices
- Strong knowledge of technical infrastructure including operating systems, networks, databases, middleware etc., to address the threats against these technologies
- Strong Knowledge of: End Point Security, Internet Policy Enforcement, Firewalls, Web Content Filtering, Database Activity Monitoring (DAM), Data Loss Prevention (DLP),Identity and Access Management (IAM)
- Proficient in reports, dashboards and documentation preparation

Work Experience

- Knowledge and experience in IT technology platforms across the IT domains.
- Technical skills to effectively perform IS security management activities/tasks in a manner that consistently achieves established quality standards or benchmarks.
- Knowledge and application of modern IS security management practices to proactively define and implement security quality improvements in line with technological and product changes.
- Knowledge and effective application of all relevant Information Security policies, processes, procedures and guidelines to consistently achieve required compliance standards or benchmarks.

2. SENIOR SYSTEMS SECURITY ANALYST (2 Posts)
Job Ref: HR: KP1/5B.2/1/3/1226

Reporting to the Principal Security Analyst, the Senior Systems Security Analyst will be responsible for Implementing, reviewing and aligning ICT Systems, Databases and Business Applications Acquisition and Development Policies, Procedures and Practice to ensure that they comply with IT industry standards to fully secure the organization's Data and Information.

The key tasks & duties for the position include;

- Assist in planning for short and long-term resources requirements for the section.

- Work with database administrators, systems developers and application owners to review and implement security controls to mitigate system security threats/risks throughout the system/program life cycle.
- Review procedures and processes to identify security control gaps in systems development, acquisition and maintenance to ensure that threats are properly identified, analyzed and mitigated.
- Participate in investigations on computer security compromises, incidents, or problems and recommend corrective actions.
- Review application, system and database logs and audit trails to identify violation to procedures and processes.
- Research on emerging threats and vulnerabilities in information security to gain awareness of the latest information security technologies and developments.
- Review version, patch management procedures and practices in all systems, and where necessary develop and implement measures to improve the same.
- Implement procedures to automate and enhance monitoring of business applications, databases and systems, including user and process activities.
- Identify and develop security and productivity-enhancing improvements and innovation.
- Coordinate security measures for information systems to regulate access to system data and information to prevent unauthorized modification, destruction, or disclosure of information.
- Train users and promote security awareness to ensure system security and to improve server and network efficiency.
- Consult with users on data and information access and processing needs, to mitigate against security violations, and programming changes.
- Recommend modification or update audit monitoring systems and solutions to incorporate new applications, databases and systems, or change individual access status
- Coordinate execution of implementation plan of system changes/upgrade between IT, user departments and outside vendors to alleviate security violations
- Perform risk assessments to identify violation or vulnerabilities to procedures and execute tests on applications to ensure that data availability, confidentiality and integrity is maintained and as well guarantee compliance to standards and process activities and advise/recommend corrective action.
- Maintain access management reports and processes to identify access events, exceptions, or trends which require investigation, remediation, or mitigation
- Contribute to the information security planning, assessments, risk analysis, risk management, certification and awareness activities for system operations.

<u>Job Specifications:</u>

- Bachelor of Science degree in Computer Science, Information Technology, Electrical & Electronics Engineering or related field.
- Certified Information Security Auditor (CISA) and/or Certified Information Security Manager (CISM) certification for Analyst IV and III respectively will be an added advantage.
- Six (6) years' experience in a similar role and organization.

Work Experience

- Experience in System vulnerability checks and threats analysis including penetration testing.
- Proficiency in computer applications as in Serve Systems administration, Database Servers, Programming and Systems analysis.
- Understanding best practices in systems security and controls.
- Good Project Management skills.

HOW TO APPLY

Interested persons should submit their applications **online** through **visiting Kenya Power website** on **http://www.kplc.co.ke**. Attach detailed Curriculum Vitae, copies of Academic and Professional Certificates and other testimonials. Please note that we may use this information to conduct background verification during the recruitment process. Quote the title of the position you are applying for and include your mobile telephone contact, email addresses to be received not later than **Wednesday,1st November 2023.**

Only candidates offered employment shall present the following clearance certificates;

- Valid Certificate of Good Conduct from the Directorate of Criminal Investigations
- Valid Clearance Certificate from Higher Education Loans Board (HELB)
- Valid Tax Compliance Certificate from Kenya Revenue Authority (KRA);
- Current Clearance from the Ethics and Anti-Corruption Commission (EACC);
- Current Report from an approved Credit Reference Bureau (CRB)

An attractive remuneration package and benefits awaits successful candidates.

Canvassing will lead to automatic disqualification.

Kenya Power is an Equal Opportunity Employer.

Kenya Power does not charge any fee at any stage of the recruitment process *(application, shortlisting, interviewing, and/or offer)*