BROADBAND SYSTEMS CORPORATION, LTD (BSC Ltd)
Remera, Kisment, Airport road KN5RD,
B.P 7229
Email: info@bsc.rw
Kigali – Rwanda

JOB ADVERTISEMENT

POSITIONS: Information Systems and Network Security Manager

1. Background:

Broadband Systems Corporation, Ltd ("BSC Ltd") is a licensed Internet Service Provider (ISP) that has been incorporated under the laws and regulations of the Republic of Rwanda. The company is engaged in the business of providing advanced Information Communication Technology ("ICT") services based on broadband connectivity.

2. Objective of the Assignment

The objective is to recruit a person for the position of Information Systems and Network Security Manager in order to achieve organization goals by defining, integrating, and upgrading comprehensive Security system architecture; managing projects and Network security.

3. Scope of Work

3.1 Description

The Information Systems and Network Security Manager is responsible for understanding and responding to threats to the security of all information, networks, and computer systems, whether on premise or cloud. The individual taking the role will monitor a variety of services and tools (including the Managed Security Service, the firewalls, third party sensor/detector/rating services, internal account activity tools, and threat information services) in order to predict, detect, and diagnose threat activity, and direct or participate in control, eradication, and restoration activities in collaboration with other team in technical department.

3.2 Responsibilities

Information Systems and Network Security Manager would be responsible for the following:

- Monitor information systems, computers and networks to detect, respond and remediate Network security threats and vulnerabilities
- Analyze, design, and facilitate capabilities, solutions, or preventative/remediation controls to protect proprietary/confidential data and systems in accordance with industry standards and regulatory/compliance requirements
- Synthesize solution design, architectural patterns, policy and regulatory frameworks, privacy considerations, and risks in the creation of holistic solutions that span technologies and capabilities

- Support the front-line defense of networks, protecting information from unauthorized access and violations. Analyze and assess potential security risks, develop plans to deal with such incidents by putting measures in place such as firewall, IPS, SIEM and encryption, monitoring and auditing systems for abnormal activity, and executing corrective actions. Prepare technical reports.
- Carry out tests on a system to expose weaknesses in security. Essentially, do everything a hacker would do, but do it on behalf of the institution that owns the network. This means will try to access information without usernames and passwords, and will try to break through whatever security applications are in place. Report findings and then suggest what upgrades/solutions to be implemented.
- Recover deleted files; analyze and interpret data linked to crime; analyzes computer logs and uncover links between events, groups and individuals through pursuit of data trails.
- Work across LINUX, Windows platforms and technologies to design holistic security designs that treat identified risks and enable strategic and/or tactical business or IT solutions
- Research/investigate emerging business application security topics, threats, capabilities, and solution options to create/update policy and governance, technology strategies, solution architecture, and vulnerability assessments
- Participate in and/or lead vendor product reviews, evaluations, demonstrations, proofs of concept and implementations
- Apply systems analysis techniques, including consultations with users to determine security specifications
- Analyze existing security systems and make recommendations for changes or improvements
- Prepare reports and action plans in the event that a security breach does occur
- Organize and conduct tests and "ethical hacks" of the existing security architecture
- Ability to use technical expertise and analytical skills to collaborate with internal and third party to ensure new hardware or solutions for the organization's network meets business and security standards
- Implement security test measurements for network vulnerability with penetration testing teams
- Implement information security framework for the organization's systems, networks and data center

3.3 Competencies

- **Analysis:** Identify and understand issues, problems and opportunities; compare data from different sources to draw conclusions.
- **Communication:** Clearly convey information and ideas through a variety of media to individuals or groups in a manner that engages the audience and helps them understand and retain the message.

- **Exercising Judgment and Decision Making:** Use effective approaches for choosing a course of action or developing appropriate solutions; recommend or take action that is consistent with available facts, constraints and probable consequences.
- **Technical and Professional Knowledge:** Demonstrate a satisfactory level of technical and professional skill or knowledge in position-related areas; remains current with developments and trends in areas of expertise.
- **Building Effective Relationships:** Develop and use collaborative relationships to facilitate the accomplishment of work goals.
- **Client Focus:** Make internal and external clients and their needs a primary focus of actions; develop and sustain productive client relationships
- **Ability to frame an architecture strategy** and gain buy-in from both business and IT executives
- **Demonstrated ability to describe non-functional requirements** and translate into architecture constraints

4. Qualifications & Experience

4.1. Educational Qualification:

Bachelor's degree in Computer Science, Information Security, or Information Systems Management

4.2. Work Experience:

- Minimum Eight (8) years of experience working daily with network or host-based threat detection technologies.
- Must be pro-active and a self-starter as this position requires a lot of independent work.
- Knowledge of networking technologies and protocols, including Ethernet, VLANs, TCP/IP and routing.
- Experience with security technologies including: Vulnerability Scanning, Firewalls & Log Analysis, Host-based detection tools, Security Event and Incident Management (SEIM), Antivirus, Network Packet Analyzers, malware analysis and forensics tools.
- Experience in analyzing audit logs, router logs, firewall logs, IDS logs and TCP/IP headers.

4.3. Certification:

At least 2 certifications among the following: CCNA, CCNP, CISSP, Sec+.

5. Reporting Arrangements

The Information Systems and Network Security will assist and report to the Senior Network Operations Manager, under the general supervision and guidance of the Chief Technical Officer.

6. Reporting requirements/deliverable:

The Information Systems and Network Security Manager will need the following reporting requirements/deliverables, but not limited to:

- Weekly reports
- Monthly work plan and progress report;
- Yearly report
- Any other Report, as required.

Interested candidates, who meet the conditions herein, should submit their letters of application accompanied with their Curriculum Vitae, copy of Degree(s) (**note that the certified documents will be required during interview**) to BSC Ltd.'s Headquarter, located in Remera, Kisment; Airport Road KN5RD at the reception desk (Ground Floor), in a sealed envelope addressed to the Chief Executive Officer of Broadband Systems Corporation, Ltd (BSC Ltd). The deadline for submission of applications is scheduled on **02nd November 2020**

Only shortlisted candidates shall be contacted.

Done at Kigali, on 23/10/2020

Mr. Christian Muhirwa
Chief Executive Officer