Job title:	Network Security Analyst
Department:	Network Planning & Engineering, Global Network Solutions Group
Location:	Worldwide, works out of the Calgary office
Supervisor:	Network and Security Team Lead

JOB DESCRIPTION

About Network Innovations:

Network Innovations is a leading provider of Satellite & Communications services including VSAT networks, Mobile broadband, Push-to-Talk and IoT solutions. NI serves clients across the globe in the Government, Media, Energy, Maritime, and Aero markets. With headquarters in Calgary, Canada, we have regional offices across North America, Europe, and Asia Pacific, and we work with over 200 partners operating globally.

Job purpose:

The Network Security Analyst is responsible for providing technical expertise to the organization to support the successful implementation, maintenance and support of the critical network and security infrastructure across NI's internal networks, NI's customer-facing PoP networks, and NI-managed customer networks.

As a member of the Network and Security team supporting operations worldwide, the Network Security Analyst will provide a mix of onsite and remote support as required, and demonstrate the skills required to secure and manage network infrastructures to protect productivity, mitigate threats, optimize costs, and build confidence in NI's security capabilities.

Duties and responsibilities:

- Responsible for the implementation, administration, documentation and continuous improvement of NI's cyber defenses across NI's internal network, PoP networks, and NI-managed customer networks.
- Ensure redundancy and stability of all critical network and security devices.
- Respond to network events and incident escalations from possible cyber-attacks, intrusions, and anomalies.
- Perform root cause analysis with vendor engineers and internal teams for incidents and recurring issues and implement permanent remediations and solutions.
- Creating queries/rules for specific searches, reports and alerts on SIEM.
- Perform vulnerability assessments and internal security audits, and regularly assess and report on NI's overall security posture.
- Manage compliance and audit-related tasks and ensure that work performed complies with cyber security and IT policies. This will include gathering evidence to

enter into our GRC systems to assist with external audits (NIST, ISO 27001, CMMC, CIS).
- Work with the cybersecurity leadership to develop company-wide best practices for IT security.
- Create and improve documentation for NI network infrastructure and update documentation as changes are made or incidents occur (change management).
- Communication with customers and users as required, keeping them informed of incident progress, and notifying them of planned changes or outages.
- Review and resolve customer troubles as escalated by internal or external facing technical teams.
- Identify cyber solutions that would be valuable to our customer base and work with commercial managers to review & develop potential solutions.
- Perform research and development and keep on top of current IT strategies and trends, and be a driver for continual improvement within the NP&E team.

Qualifications:

- At least 8 years' experience in Network and Security Operations with at least 5 years of supporting Enterprise Networks.
- Experience in multi-national operations.
- Personal Characteristics: problem solving, ability to work under pressure, confidential and ethical, results driven, customer focus, structured, and a team player.
- Strong troubleshooting skills and the ability to break down and solve complex problems.
- Implementing cybersecurity and networking solutions including routing, switching, wireless, firewalls, remote access, access control, VPN, zero-trust network concepts.
- Intermediate knowledge in Dynamic routing protocols - BGP, OSPF.
- Knowledge of SIEM and EDR Solutions.
- Knowledge of Vulnerability Management Solutions.
- Knowledge of Identity and Access Management.
- CCNA level certification.
- Palo Alto Networks Certified Network Security Engineer (PCNSE) is an asset.
- Knowledge of cyber security frameworks (e.g., NIST, ISO 270001 or CMMC).
- Cyber Security Certification (e.g. CompTIA Security+, CISSP, CEH) is an asset.
- Strong written and verbal communication.
- Passion and pride in your work results.
- A willingness to embrace and live the core values of Network Innovations.

Working conditions:

This position will normally have office hours of 8am to 5pm local time, 5 days a week. However, the incumbent must be available 24/7 x 365, within reason, to address issues in the IT environment. The position operates in a professional office environment. This role routinely uses standard office equipment and software.

Physical requirements:

An ability to travel and on a global basis. A valid passport without restrictions. Sitting and using a computer for extended periods of time.

Disclaimer Statement: This job description lists the essential functions of the position and is not intended to include every job duty and responsibility specific to a position. An employee may be required to perform other related duties not listed above provided that such duties are characteristic of that classification**.**