Duty Location: **Brussels, BEL**

JOB DESCRIPTION

Principal Analyst (Cyber Security – Gateway)

Directorate of CIS Support Units – CSU Brussels
Grade: **G12**

This is a position within the NATO Communications and Information Agency (NCI Agency), an organization of the North Atlantic Treaty Organization (NATO).
The NCI Agency has been established with a view to meeting to the best advantage the collective requirements of some or all NATO nations in the fields of capability delivery and service provision related to Consultation, Command & Control as well as Communications, Information and Cyber Defence functions, thereby also facilitating the integration of Intelligence, Surveillance, Reconnaissance, Target Acquisition functions and their associated information exchange.
The Directorate of CIS Support Units (DCSUs) leads CIS Support Units (CSUs) business area and oversee all CSUs, along with the Operations and Exercises Service Line. DCSU enables end-to-end CIS services by directing the Agency's local units at each command location through the installation, operation, maintenance and support of the full range of CIS capabilities. The CSUs play an integral role in the delivery of catalogue and non-catalogue services to the Agency's customers.
DCSUs also commands the Agency's Operations and Exercises team. This team is the Agency's interface for supplying the Command and Control Catalogue of Services to customers that are planning and/or executing operations and exercises. The Operations and Exercises team ensures that the Agency's responsibilities to deployed operations are met in line with arrangements for Command and Control, agreed Service Level Agreements and possible additional resources received through the Customer Request Form and Price Proposal (PP) process.
NCI Agency CIS Support Unit (CSU) Brussels, located in Brussels (BEL) is the primary Information, Communications and Technology (ICT) service provider for 24/7 support to the Secretary General, the International Staff (IS), the International Military Staff (IMS) and other Customers in the NATO Headquarters in Brussels. CSU Brussels enables end-to-end CIS services as it installs, operates, maintains and supports the full range of CIS capabilities during peacetime, crisis and war throughout its allocated Area of Responsibility (AOR) and as otherwise directed.
The Cyber Security Section (CSS) performs a broad range of cyber security activities as delegated by the Cyber Security Service Line and under the direct command and control of the CSU commander. These activities include advise to the CSU Commander about cyber security policies and risk assessments, acting as the integration point of contact for implementation of cyber security new capability fielding initiatives, provision of Level One cyber security expertise and lifecycle support as required, verification of the implementation of security settings and change management controls at the local level, assessing and re-distributing cyber security alerts to CSU users and leadership, administering endpoint security services. Furthermore the CSS supports the incident management process, provides on-site support, reports in direct coordination with the Cyber Security Service Line and implements remediation measures. While developing situational awareness when monitoring assigned systems and portions of the network. CSS also performs crypto key-management for itself and Customers in the assigned Area of Responsibility within policy guidelines and serves as the point of contact for new cryptographic equipment installation and implementation. CSS also performs cryptographic management services for the CSU and customers in the assigned Area of Responsibility.This position is located in the team responsible for managing endpoint security systems (anti-virus, data loss protection, host firewalls, application control, etc).

Duties:

Under the direction of the Section Head the incumbent will perform duties such as the following:

- Manage cyber security gateway systems (firewalls, proxies, email gateway, VPNs, etc);
- Manage endpoint security systems (anti-virus, data loss protection, host firewalls, application control, etc);
- Operate log consolidation systems and support log data analysis;
- Assist in managing public key infrastructure in accordance with NATO, ACO and Agency directives;
- Initiate and maintains liaison with other internal units, Service Lines and other Security Authorities;
- Assist with cyber security advice and provide Level 1, Level 2 support as required;
- Execute the security incident management process and advise on improvements;
- Support vulnerability assessments and Security Testing and Verification (ST&V) plans within policy guidelines, and as directed;
- Responsible for monitoring of assigned systems and portions of the networks, including support to local cyber security training and awareness programs;
- Co-ordinates assistance to L3 support, as required, in respect to event analysis and interpretation;
- Periodically provide on demand support outside of business hours that could require working on site;
- Work on own initiative with limited supervision, and possibly lead others as required;
- Plan, manage, coordinate and conduct work to meet quality targets;
- Take initiative to investigate and resolves issues in a systematic approach;
- Assist superiors and recommends solutions;
- Deputize for higher grade staff, if required;
- Perform other duties as may be required.

Experience and Education:

- Higher vocational training in a relevant discipline with 3 years post-related experience, or a secondary educational qualification with 5 years post-related experience;
- Experience of cyber security activities in large, complex and possibly classified ICT environments with 2.000+ end-user devices;
- Strong network knowledge;
- Ability to create documentation including diagrams and processes;
- Good communication skills, both verbal and written;
- ITIL v3 certification(s);

Desirable Experience and Education:

- Experience working with cyber security gateway systems (firewalls: Palo Alto and Juniper, proxies, email gateway, VPNs, etc);
- Possession of at least one security certification (i.e., ISC, EC-Council, SANS) highly desirable;
- Completion of the NATO Security course;
- Prior experience of working in an international environment comprising both military and civilian elements;
- Knowledge of NATO responsibilities and organization, including ACO and ACT.

Language Proficiency:

- A thorough knowledge of one of the two NATO languages, both written and spoken, is essential and some knowledge of the other is desirable.
- **NOTE:** Most of the work of the NCI Agency is conducted in the English language.

Competencies or Personal Attributes:

- Relating and Networking - Easily establishes good relationships with customers and staff; relates well to people at all levels; builds wide and effective networks of contacts; uses humour appropriately to bring warmth to relationships with others;

- Delivering Results and Meeting Customer Expectations -- Focuses on customer needs and satisfaction; sets high standards for quality and quantity; monitors and maintains quality and productivity; works in a systematic, methodical and orderly way; consistently achieves project goals;
- Adapting and Responding to Change -- Adapts to changing circumstances; tolerates ambiguity; accepts new ideas and change initiatives; adapts interpersonal style to suit different people or situations; shows an interest in new experiences;
- Achieving Personal Work Goals and Objectives -- Accepts and tackles demanding goals with enthusiasm; works hard and puts in longer hours when it is necessary; seeks progression to roles of increased responsibility and influence; identifies own development needs and makes use of developmental or training opportunities.