Duty Location: **Mons, BEL**

JOB DESCRIPTION
Engineer (Cyber Security)
NATO Cyber Security Centre– Infrastructure Branch

Grade: **G15**

This is a position within the NATO Communications and Information Agency (NCIA), an organization of the North Atlantic Treaty Organization (NATO).

The NCI Agency has been established with a view to advantageously meeting the collective requirements of NATO nations in the fields of capability delivery and service provision related to Consultation, Command & Control, as well as Communications and Information / Cyber Defence functions; thereby, facilitating the integration of Intelligence, Surveillance, Reconnaissance, Target Acquisition functions and their associated information exchange.
The NATO Cyber Security Centre (NCSC) is responsible for planning and executing all lifecycle management activities for cyber security. In executing this responsibility, NCSC provides specialist cyber security-related services covering the spectrum of scientific, technical, acquisition, operations, maintenance, and sustainment support, throughout the lifecycle of NATO Communications and Information Systems (CIS). The NCSC enables secure conduct of the Alliance's operations and business in the context of NATO's C4ISR. The NCSC provides cyber security services to NCI Agency customers and users, as well as to all other elements of the Agency; this includes all Service Lines, Programme Offices, CIS Support Units/Elements, and the Agency Ops Centre. The NCSC is responsible for providing the bread spectrum of services in the following specialist security areas: CIS Security, Cyber Defence, Information Assurance, Computer Security and Communications Security. In executing its responsibilities, the NCSC provides support to the development and implementation of cyber security-related policy, strategy, and provides lifecycle security risk management services for all NATO CIS. The NCSC leads in the development of new capabilities and innovation in cyber security. The NCSC incorporates and provides specialist services to prevent, detect, respond to and recover from cyber security incidents.

The Infrastructure (INFRA) Branch delivers a suite of enabling services in the specific areas of Cryptography, Identity Management, Technical Services (supporting CS Operations) and CIS Protection. These services include integration and validation of NATOs crypto solutions, lifecycle management of cryptographic equipment and keys, operation and logistic support for NATO-wide online and offline cryptographic equipment, identity management services, gateway services, specialized enterprise-wide CS infrastructure (including NCIRC elements), applications, implementation, configuration and management of NATO Enterprise-wide endpoint security software.

The Security Tools Management Services (STMS) Section is responsible for delivering centrally managed security tools for internal and external users, as well as providing expert guidance for the implementation, configuration and management of NATO Enterprise-wide endpoint security software. The services, mainly in the form of Software-as-a-Service, provided by the section are enabling the core services delivered by NCSC branches as well as the endpoint protection of NATO static, Alliance Operations, and Missions footprints.

Duties:

Under the direction of Head STMS, Data Lead Engineer STMS or a delegated authority, the incumbent will perform duties such as the following:

– Act as one of the main engineers and Subject Matter Expert (SME) for SIEM and LogA services within the Cyber Security Data team;
– As the SME, you will provide advice and technical assistance to other stakeholders, maintain technical expertise, awareness, and developments in related new technologies, and provide technical contributions to any projects related to the data security systems;
– Be responsible for management and further development of the data security systems;

- Following ITIL standards, provide support to Operations and Service Delivery management covering all stages of the data security systems lifecycle (e.g. Service Design, Transition, Operations, Change Management and Continual Service Improvement);
- Ensure that data security systems are installed, configured, and operating correctly and in line with dependencies with others systems or applications required;
- Ensure that all system components are continuously monitored and take appropriate technical and non-technical actions for solving detected issues;
- Ensure that data security systems operate within any KPI's, as defined in Service Level Agreements with NCSC customers;
- Support integration with external tools and any associated activities;
- Proactively identify and propose system improvements to ensure an up-to-date and stable environment. Justify business needs, prepare documentation and implementation plan for the Change Management Board. Implement the approved changes following co-ordination with other stakeholders;
- Coordinate with service delivery managers, end users and other stakeholders in support of related services; communicate with other NATO entities as well as industry partners where required;
- Develop and maintain documentation guidelines, standard operating procedures, system and service design documents and other relevant documentation that support management of the data security systems;
- Create technical and/or executive level reports as required; organise and deliver presentations and briefings for various audience up to NATO executive level;
- Deputize for higher grade staff, if required;
- Perform other duties as may be required.

NOTE: This role is not a Cyber Security analyst; utilisation of cyber tools (conducting forensic investigations, malware or vulnerability analysis) ***is not*** *considered to be part of standard duties.*

Experience and Education:

- A minimum requirement of a Bachelor's degree at a nationally recognised/certified University in a related discipline and 2 years post-related experience. Exceptionally, the lack of a university degree may be compensated by the demonstration of a candidate's particular abilities or experience that is/are of interest to NCI Agency, that is, at least 6 years extensive and progressive expertise in duties related to the function of the post;
- At least 1 year of extensive practical experience as Splunk administrator in large enterprise environment (deployment, installation, configuration and maintenance);
- Practical experience in designing Splunk based solutions;
- Practical experience of Splunk Enterprise security, Phantom and UBA;
- At least 2 years and expert level experience related to SIEM/LogA management activities;
- Demonstrable experience of analysing and interpreting system, security and application logs in order to diagnose faults and spot abnormal behaviours;
- Practical hands-on experience in systems and tools administration, especially Linux environment;
- Comprehensive knowledge of the principles of computer and communication security, networking, and the vulnerabilities of modern operating systems and applications;
- Practical skills in writing Bash, Python or Ansible scripts to support repetitive tasks automation;
- Linux system and application administration and troubleshooting;
- Solid understanding of regular expressions;
- Ability to develop clear and concise technical documentation, including procedures;
- Demonstrable ability to work autonomously and proactively, to understand the chain of command and to follow internal processes;
- Good communication abilities, both written and verbal, with the ability to clearly and successfully articulate complex issues to a variety of audiences and teams.

Desirable Experience and Education:

- Extensive practical experience (as system administrator) with Splunk Enterprise security, MicroFocus ArcSight, Phantom and UBA;
- Experience in GIT;

- Hands-on experience with Ansible as an automation technology;
- Proficient with SIEM content creation – correlation rules, reports, dashboards;
- Experience in creation/modification of custom parsers or flex connectors;
- Understanding the Indicator of Compromise (IOC) concept and experience in integration of Threat Intel feeds and IOCs with SIEM platform;
- Software engineering including programming and/or scripting knowledge (python, shell scripting, PowerShell);
- Prior experience automating interactions between systems using APIs;
- A solid understanding of Information Security Practices; relating to the Confidentiality, Integrity and Availability of information (CIA triad.);
- Prior experience as a user of SIEM and Log aggregation systems;
- ITIL Service Management certifications;
- Experience in developing Splunk Applications;
- Content management experience in Splunk, especially Enterprise Security and Advanced Search and Reporting;
- Hands-on experience with network infrastructure and virtualised environments (preferably VMWare).
- Industry leading certification in the area of Cyber Security such as CISSP, CISM, MCSE/S, CISA, GSNA, SANS GIAC and CFCE;
- Previous experience working for Cyber Security related organisations (CERTs, security offices);
- Previous experience 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:

- 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.
- Adhering to Principles and Values - Upholds ethics and values; demonstrates integrity; promotes and defends equal opportunities, builds diverse teams; encourages organisational and individual responsibility towards the community and the environment.
- 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.