JOB DESCRIPTION

Post Details:			
Post Title:	**Cyber Security Defender**	Organisational Element:	NCSC
Military/Civilian:	Civilian	Location:	Mons, Belgium (BE)

Organisation context:

This is a position within the NATO Communications and Information Agency (NCIA), an organization of the North Atlantic Treaty Organization (NATO).
To strengthen the Alliance through connecting its forces, the NCIA delivers secure, coherent, cost effective and interoperable communications and information systems in support of consultation, command & control and enabling intelligence, surveillance and reconnaissance capabilities, for NATO, where and when required. It includes IT support to the Alliances' business processes (to include provision of IT shared services) to the NATO HQ, the Command Structure and NATO Agencies.

Organisational Element Statement of Functions:

The NATO Cyber Security Centre (NCSC) delivers full lifecycle cyber services to enable the secure execution of NATO's consultation, operations, and missions and enhance the Alliance's collective cyber defence.

As its principal provider of cyber services, the NCSC makes NATO more resilient to cyber threats, protecting and defending Communications and Information Systems (CIS) through centralized and round-the-clock services. The NCSC also leads the implementation of new cyber capabilities within NATO and supports other Business Areas in the implementation and delivery of cybersecurity projects and services. In addition to delivering services and managing projects, the NCSC also provides the technical hands-on-keyboard experts for the conduct of Defensive Cyber Operations (DCOs).

Core activities include, inter alia, technical design, guidelines development, accreditation support, cybersecurity capabilities management, vulnerability assessment and remediation support, operating the NATO Public Key Infrastructure, malicious activity detection, threat hunting, incident response, information sharing, TEMPEST zoning, management of cryptographic systems, penetration testing, purple and red teaming, and defensive cyber operations including maintaining a rapid reaction team. It also tracks research and pursues innovation in cyber.

The NCSC is the centre of technical expertise for cyber within the Alliance and leads information sharing and collaboration initiatives at the technical level within the Alliance and with external stakeholders.

The NCSC is part of the nucleus of the NATO Integrated Cyber Defence Centre (NICC).

Job role description:

A Cyber Security Defender is responsible for protecting an organization's information, users, computer networks and systems from unauthorized access and cyber-attacks. They execute Cyber Defense Operations on these networks, monitor them for security breaches, detect and respond to cyber security incidents,

leverage cyber threat intelligence to adapt security measures and execute threat hunts. They also stay up to date with the latest security technologies and trends to ensure that the organization's security infrastructure is always current and effective.

Duties and Responsibilities:

Information security:

- Provides guidance on the application and operation of elementary physical, procedural and technical security controls.
- Explains the purpose of security controls and performs security risk and business impact analysis for medium complexity information systems.
- Identifies risks that arise from potential technical solution architectures.
- Designs alternate solutions or countermeasures and ensures they mitigate identified risks.

Information assurance:

- Performs technical assessments and/or accreditation of complex or higher-risk information systems.
- Identifies risk mitigation measures required in addition to the standard organisation or domain measures.
- Establishes the requirement for accreditation evidence from delivery partners and communicates accreditation requirements to stakeholders.
- Contributes to planning and organisation of information assurance and accreditation activities.
- Contributes to development of and implementation of information assurance processes.

Specialist advice:

- Provides detailed and specific advice regarding the application of their specialism to the organisation's planning and operations.
- Actively maintains knowledge in one or more identifiable specialisms.
- Recognises and identifies the boundaries of their own specialist knowledge.
- Where appropriate, collaborates with other specialists to ensure advice given is appropriate to the organisation's needs.

Additional duties for this post:

- Act as one of the main engineers and Subject Matter Expert (SME) for SIEM and Log collection services.
- 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.
- 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.

Education, Experience and Training (essential):

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. Or 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 NCIA, that is, at least 6 years extensive and progressive expertise in duties related to the function of the post.

Experience:

- At least 1 year of extensive practical experience as SIEM administrator in large enterprise environment (deployment, installation, configuration and maintenance).
- Hands-on experience in the design and maintenance of distributed Splunk architectures.
- At least 2 years and expert level experience related to SIEM and Log collection management activities with Splunk Enterprise.
- 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.
- Solid Linux system and application administration and troubleshooting skills.
- 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.

Education, Experience and Training (desirable):

Education:

- Master's Degree in Cyber Security or IT Security-related discipline.

Experience:

- Extensive practical experience (as system administrator) with Splunk Enterprise security, Splunk SOAR and Splunk UBA.
- Practical experience with Git software.
- Hands-on experience with Ansible as an automation technology.
- Experience in creation/modification of custom parsers.
- Software engineering including programming and/or scripting knowledge (python, shell scripting, PowerShell).
- Prior experience automating interactions between systems using APIs.
- Hands-on experience with Cribl Stream for data collection, routing, filtering, transformation.
- A solid understanding of Information Security Practices; relating to the Confidentiality, Integrity and Availability of information (CIA triad.).
- 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).
- Previous experience working for Cyber Security related organisations (CERTs, security offices).
- Experience with log collection in cloud environment such as Azure or AWS.

Training/Certifications:

- Possessing industry leading certification in the area of Cyber Security such as CISSP, CISM, CISA, GSNA, and SANS GIAC.
- Possessing Splunk certifications such as Splunk Admin, Splunk Power User, Splunk Architect.

Behavioural competencies:

- *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.

Language:	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 NCIA is conducted in the English language.