JOB DESCRIPTION

Post Details:			
Post Title:	**Cyber Security Defender**	Organisational Element:	NCSC
Military/Civilian:	Civilian	Location:	Mons/BEL

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.
- Investigates suspected attacks and supports security incident management.

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:

- The incumbent will be responsible for the administration, maintenance, and continuous improvement of enterprise cyber defence tools that support network security monitoring, threat detection, and threat hunting.
- Acts as a subject matter expert for network visibility, security monitoring, and packet capture capabilities, ensuring platforms remain reliable, effective, and aligned with organizational security objectives.

Security Tool Operations & Lifecycle Management:

- Deliver and maintain the network visibility and security monitoring capabilities.

- Act as a subject matter expert for the operation, configuration, and lifecycle management of security monitoring and packet capture technologies.
- Manage the lifecycle of security monitoring platforms, including deployment, configuration, maintenance, upgrades, obsolescence management, and decommissioning.
- Configure, maintain, and optimize monitoring, traffic aggregation, and packet capture technologies to support reliable data collection and analysis.
- Monitor platform health, availability, data quality, retention, storage utilization, and operational performance.
- Identify and address visibility gaps that may impact threat detection or security operations.
- Maintain accurate documentation, architecture diagrams, inventories, operational procedures, and support information.
- Troubleshoot Linux, network, connectivity, performance, and data collection issues across the security monitoring environment.

Continuous Improvement:

- Support the design and implementation of security monitoring solutions.
- Support integration with wider security operations, analytics, and incident management capabilities.
- Work with security analysts, detection engineering, and other stakeholders to improve monitoring coverage and support evolving detection requirements.
- Conduct capacity planning and scalability assessments to support future growth.
- Identify operational risks, improvement opportunities, and enhancements to increase reliability, visibility, and efficiency.
- Support compliance, audit, and assurance activities related to cyber defense technologies.

Stakeholder Engagement & Project Support:

- Provide subject matter expertise and technical guidance on security monitoring, network visibility, packet capture, and data collection requirements.
- Support projects and initiatives by ensuring monitoring and visibility requirements are considered during design, implementation, and service transition.
- Support cabling, deployment planning, and site survey activities related to security monitoring and network visibility infrastructure.
- Coordinate maintenance activities, vendor support engagements, and communications relating to platform status, risks, and improvement opportunities.
- If requested, participate in cyber defence related exercises supported by NCIA.
- Support the Defend Branch service delivery in the context of NCIA Enterprise Service Delivery Model and NCIA Customer Funded regime.
- Deputize for higher grade staff, if required.
- Performs 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 NCI Agency, that is, at least 6 years extensive and progressive expertise in duties related to the function of the post.

Experience:

- Expert knowledge of network security monitoring, cyber defence operations, and enterprise security monitoring environments.
- Extensive hands-on experience supporting large-scale, distributed security monitoring deployments across multiple networks, sites, segments, or data centres.
- Hands-on enterprise experience with security monitoring and packet capture platforms such as Cisco Firepower, Corelight, and NetWitness.
- Proven experience in platform health monitoring, performance monitoring, capacity management, troubleshooting, and operational governance.
- Strong hands-on experience with network visibility, traffic aggregation, packet brokers, packet capture, and related monitoring technologies.
- Advanced understanding of enterprise networking concepts, protocols, architectures, and data flows.
- Linux and network troubleshooting experience, including connectivity, packet flow, interface, performance, and system-level diagnostics.
- Practical experience supporting cabling, site surveys, and physical deployment activities for monitoring or network visibility infrastructure.
- Strong knowledge of security telemetry collection, event correlation, threat detection, and threat hunting concepts.

Education, Experience and Training (desirable):

Education:

- Hold a university degree in Cyber Security or IT Security-related discipline.

Experience:

- Experience designing large-scale security monitoring and network visibility architectures.
- Experience integrating security monitoring tools with SIEM and SOAR tooling.
- Experience with automation, scripting, or orchestration.
- Experience supporting major platform upgrades, migrations, refreshes, or service transition activities.
- Prior experience in working in an international environment comprising both military and civilian elements.
- Knowledge of NATO responsibilities and organizational structure, including ACO and ACT.

Training/Certifications:

- Hold relevant certifications such as the ones from GIAC, ISC2, ISACA or other recognized certification programmes, ideally with emphasis on IT security.

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 NCI Agency is conducted in the English language.
Work Environment:	Normal office environment. Normal working hours 0830-1730. On-call duties may be required after working hours, on weekends or holidays. The incumbent may be required to perform duties elsewhere within the organization as directed. The incumbent may be required to work on 12 hours pattern during weekdays but not exceeding an average of 38h per week. In case of an enterprise-level Cyber Incident, the incumbent may be required to work extended hours and on shifts, including nights and weekends, to provide a 24/7 Cyber Security Incident Response.