JOB DESCRIPTION

Post Details:

Post Title:	**Senior Cyber Security Defender**	Location:	Mons, BEL
Military/Civilian:	Civilian		

Organisation context:

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

To strengthen the Alliance through connecting its forces, the NCI Agency 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) 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 and operational support to NCI Agency customers and users, as well as to all other elements of the Agency; this includes all Business Areas, Programme Offices, CIS Support Units/Elements, and the Agency Ops centre. The NCSC is responsible for providing the broad spectrum of services in the following specialist security areas: Cyber Security, Cyber Defence, Defensive Cyberspace Operations and support to Allied operations and Missions (AOM). In executing its responsibilities, the NCSC provides lifecycle security risk management services for all NATO CIS. The NCSC leads in the development of the new capabilities and innovation in Cyber Security. The NCSC incorporates and provides specialist services to prevent, detect, respond to and recover form cyber security incidents. The NCSC is evolving to include aspects of mission assurance into its mission to ensure continued success of NATO operations.

Job role description:

A Senior 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 Defence 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. They also provide guidance and training to other members of the security team.

The Senior Cyber Security Defender (SCSD) is NATO's main cyber-security incident coordinator. Coordination responsibilities include:

- Downward coordination – advice and recommendations to local CIS Security Officers and staff.
- Lateral coordination – between teams within NCI Agency, NCSC, NATO stakeholders, Security Accreditation Authorities, Allied Command Operations Cyber Operations Centre, and other cyber-related organisations.
- Upward coordination – offering technical SME advice to decision makers at the strategic and political level, such as the NATO Office of Security, Office of the Chief Information Officer, and Cyber Threat Analysis Branch.
- National coordination – in relation to sharing incident related information between NATO and National points of contact.

Additionally, the SCSD is a team member of the CSIRT, which is responsible for leading Cyber Security Incident Response activities across NATO organisations, networks and CIS. This includes liaising with internal SMEs across the NCSC, providing a holistic view of cyber-security incidents for NCSC management, and participating in major incidents, such as a cyber-incident task force when called upon.

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:

- Interprets information assurance and security policies and applies these to manage risks.
- Provides advice and guidance to ensure adoption of and adherence to information assurance architectures, strategies, policies, standards and guidelines.
- Plans, organises and conducts information assurance and accreditation of complex domains areas, cross-functional areas, and across the supply chain.
- Contributes to the development of policies, standards and guidelines.

Specialist advice:

- Provides definitive and expert advice in their specialist area.
- Actively maintains recognised expert level knowledge in one or more identifiable specialisms.
- Oversees the provision of specialist advice by others.
- Consolidates expertise from multiple sources, including third-party experts, to provide coherent advice to further organisational objectives.
- Supports and promotes the development and sharing of specialist knowledge within the organisation.

Additional duties for this post:

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

- Provision of 24/7 Cyber Incident Response (TRIAGE, Contain, Eradicate, Recover) activities, during normal working hours and on-call duties, including weekends and holidays on all NATO networks.
- Deliver technical and procedural co-ordination, support and assistance in respect of Cyber Incident Response to Cyber Incident Task Force (CITF) lead and members, NATO CIS Operating Authorities (CISOA) or other similar bodies as directed, including but not limited to, NATO Nations, Partner Nations, non-Governmental Organisations and Industry partners.
- Deliver guidance and provide support on NCI Agency Cyber Incident Response topics to and in coordination with the Enterprise Service Operations Centre (ESOC).
- Lead, be a member of, or support a CITF, a Cyber Security Response Team (CSRT), Cyber Defence Rapid Reaction Team (CD RRT) or Defensive Cyber Operations (DCO) team designated to provide Cyber Incident Response or DCO happening on one or multiple physical locations, including NATO Alliance Operations and Missions.
- Deliver Cyber Incident reporting activities in support of NATO CIS, reporting Security Incidents to the appropriate NATO Stakeholders as required.
- Identification and Sharing of technical Indicators of Compromise, Tactics, techniques and procedures (TTPs) or cyber incidents' contextual information with the other NATO stakeholders, the NATO nations and our different partners, in accordance with our sharing agreements, the NATO information management policy and the need-to-know principle.
- Lead Coordination activities related to Cyber Security Incident Management, tasking and/or requesting support from SMEs across the NCSC.
- Assessing the full scope of technical analysis provided by SMEs, sites, users, and other NATO bodies in relation to Cyber Security incidents.
- Provide appropriate and specific Courses of Action to contain, mitigate, and eradicate cyber security threats within the NATO enterprise environment.
- Analysis, interpretation and dissemination of Security Advisories and Threat Intelligence Reports from NATO Nations, Partner Nations, non-Governmental Organisations and Industry partners.
- Present, redact, review and prepare reports, recommendations and presentations to the CITF, the Cyber Incident Decision Making Group (iCDMG), the Security Authorities and NATO IA communities on all aspects of Cyber Incident Response.
- Research to identify, document and implement improvements to the Cyber Incident Response activities in order to enhance and optimise current best practice to meet new and developing threats.
- Production of Standard Operating Procedures and Instructions covering all aspects of Cyber Incident Response activities in accordance with NCSC's IKM governance and tools.
- Support the CSIRT Management in the context of NCI Agency Enterprise Service Delivery Model, NCI Agency Customer Funded regime, and resource (people) management.
- Deputize for higher grade staff as 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 3 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 10 years extensive and progressive expertise in duties related to the function of the post.

Experience:

- Excellent ability to recognise when an IT network/system has been attacked, be able to take immediate

action to limit damage and to escalate the event to higher authority.

- Excellent ability to analyse complex situations under time pressure, providing relevant prioritized courses of action, distributing the tasks to colleagues, tracking the completion of them and interpreting their results to reassess the course of action.
- Excellent communications skills and reporting experience with capacity to communicate to different types of audience (senior executive, middle management, technical and non-technical).
- Comprehensive understanding of the principles of Computer and Communication Security, networking, and the vulnerabilities of modern operating systems and applications acquired through a blend of academic or professional training coupled with practical professional experience.
- Recent practical, hands-on experience of Intrusion Detection and Incident Response (TRIAGE, Contain, Eradicate, Recover) in an enterprise-level Computer Emergency Response Team.
- Very good experience in interpreting the results of CIS Technical Security/Vulnerability Assessments.
- Very good experience in the implementation and integration of Cyber Security protective measures.

Education, Experience and Training (desirable):

Education:

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

Experience:

- In-depth knowledge of potential security event sources and their interpretation and analysis in support of the incident detection and handling processes.
- A deep understanding of the MITRE ATT&CK framework and its applicability in executing cyber incident response.
- Practical experience in the management and the professional development of less experienced incident handling staff.
- A deep understanding of the management of CIS Service Delivery, ideally following ITIL framework.
- Prior experience of working in an international environment comprising both military and civilian elements.
- Knowledge of NATO responsibilities and organizational, including ACO and ACT.

Training/Certifications:

Hold relevant certifications such as Certified Information Systems Security Professional (CISSP), SANS GIAC/GCIH or GIAC/GCIM.

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.

- *Deciding and Initiating Action* - Takes responsibility for actions, projects and people; takes initiative and works under own direction; initiates and generates activity and introduces changes into work processes; makes quick, clear decisions which may include tough choices or considered risks.