



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 (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 NCIA 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 from 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 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.

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:

Under the direction of the Section Head of the Cyber Threat Investigation Section (CTIS), the incumbent will perform duties such as the following:

- Provide technical and expert support for to the 24/7 Cyber Security Incident Response Team's processes, during normal working hours and on-call duties, including weekends and holidays.
- Support Cyber Security Incident Response/Threat Hunting Team covering one or multiple physical locations, including NATO Alliance Operations and Missions.
- Plan and execute both static and dynamic code and Malware analyses/reverse-engineering and capture the results in a report which covers the technical aspects as well as the "so what?" for the decision makers and executives.
- Develop and Maintain the Digital/Network Forensics and Malware/code analysis capabilities on deployable kits to support Cyber Security Incident Response and Threat Hunting.
- Develop tools, scripting, automation and integrations to automate activities as much as possible, mostly using Python and PowerShell.
- Conduct forensic investigations and malware analysis within cloud-based or hybrid networking environments.
- Identify and share technical Indicators of Compromise with the other NATO stakeholders, the NATO nations and our different partners, in accordance with our sharing agreements.
- Write and review Standard Operating Procedures/Instructions covering all aspects of Digital Forensics and Malware Analysis.
- Interact with security vendors to submit them with undetected malware samples in order to obtain updates of their malware definitions, or to produce custom delta signatures to accurately detect threats in submitted samples.
- Interact with other NATO stakeholders to have custom Host or Network Intrusion Detection rules created based on the extraction of malware artefacts.
- 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:

- Extensive knowledge of malware analysis techniques and technologies.
- 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.

- Practical experience with cyber security in cloud-based environments.
- Proficiency in assessing security vulnerabilities of operation systems and software.
- Practical experience and knowledge of malware analysis and malware detection.
- Practical experience in the analysis of digital forensic artefacts in the context of cyber security.
- Good knowledge of the principles of computer and communications security, networking, and vulnerabilities of modern operating systems and applications.
- Good understanding of the MITRE ATT&CK framework and its applicability in Cyber.
- Good practical experience in Windows, Linux and VMware system administration.
- Good knowledge of cyber security incident handling.
- Practical experience in scripting (Python, PowerShell).

Education, Experience and Training (desirable):

Education:

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

Experience:

- Experience in using cyber information sharing platforms (e.g. MISP or commercial ones).
- Experience in conducting Digital Forensics and/or Malware Reverse-Engineering or Analysis on mobile devices.
- 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.