JOB DESCRIPTION

Post Details:

Post Title:	**Section Head Cyber Threat Investigation**	Organisational Element:	COO/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 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.

Job role description:

The incumbent must be a dynamic and results-driven professional to lead and integrate the functions of a CTIS section head, Service Delivery Manager, and Enterprise Cyber Incident Investigator into a unified, managerial role. The incumbent is in charge of leading a team delivering both NCSC Malware and Forensics (MAL&FOR) Analysis service and Threat Hunting Service. The incumbent is responsible for ensuring these services adequately support NATO Cyber Incident and Risk Management processes, overseeing activities and resources, managing the financial and operational aspects of the CTIS section. If required, the incumbent must be able to spearhead technical response in case of enterprise-level cyber incidents. The ideal incumbent will combine technical expertise, strong managerial skills, and service supplier mind-set to optimize timely threat actor activity detection and identification against NATO CIS.

Duties and Responsibilities:

Information security:

- Provides advice and guidance on security strategies to manage identified risks and ensure adoption and adherence to standards.
- Contributes to development of information security policy, standards and guidelines.
- Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems.
- Investigates major breaches of security, and recommends appropriate control improvements.
- Develops new architectures that mitigate the risks posed by new technologies and business practices.

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:

The Cyber Threat Investigation Section (CTIS) Leadership:

- Direct and supervise the delivery of efficient and effective Malware and Forensics Analysis and Threat Hunting on NATO networks.
- Ensure timely consumption of cyber threat intelligence.

- Ensure timely production of cyber threat information as output of MAL&FOR and Threat Hunt processes.
- Direct and supervise Cyber Threat Information Sharing with relevant stakeholders in support of incident response, risk management and threat assessment processes.
- Lead a team of Malware, forensics analysts and threat hunters ensuring continuous training and professional development.
- Provide authoritative and expert advice and direction on the operation of the section and its evolution.
- Promote and maintain liaison with NATO Intelligence on Cyberspace Community-of-Interest and the NATO Counter-Intelligence community.
- Promote a culture of collaboration, continuous improvement, innovation, and excellence across teams.
- Maintain and improve MAL&FOR and threat hunting processes and supporting technologies.
- Develop and implement CTIS adaptation and evolution to accomplish NCSC organisational goals.
- Represent NCSC DEFEND branch in high-level meetings, conferences, and committees.

Business Management:

- Act as Service Delivery Manager for both NCSC Malware and Forensics Analysis service and Threat Hunting services, ensuring the cost effective delivery of the services in accordance with the contracted SLAs and OLAs.
- Develop and maintain the CTIS business execution plan, ensuring optimal allocation of resources for operations, continuous service improvement and key initiatives.
- Foster cost efficiency and innovation including through outsourcing/collaboration with stakeholders and industry partners.
- Prepare reports and dashboards providing insights on the service performance.
- Build and maintain relationships with all relevant NATO and non-NATO stakeholders, including IT teams, and third-party vendors.
- Support and initiate changes to align CTIS priorities with organizational goals.
- Manage daily business activities and attend management coordination meetings.
- Deputize for higher grade staff or within management chain when required.
- Performs other duties as may be required.

Enterprise Cyber Incident Investigator (ECII):

- Lead technical investigation of NATO Enterprise cyber security incidents in line with the NATO Enterprise Cyber Incident Response Plan (CIRP).
- Provide authoritative and expert advice on technical response to cyber security incidents.
- Attend and provide technical support to NATO Cyber Incident Task Forces (CITFs) and different boards.
- Support and review post-incident reports with actionable recommendations on lessons identified.
- Collaborate with Media, Legal or Acquisition teams to address potential contractual or legal implications of cyber incidents.

Education, Experience and Training (essential):

Education:

A Master’s degree at a nationally recognised/certified University in a related discipline and 5 years post-related experience. Or a Bachelor’s degree with 8 years post related experience.

Experience:

- Significant knowledge in technologies and processes supporting Malware and Forensics activities.
- Significant knowledge in technologies and processes supporting Cyber Threat Hunting activities.

- Experience in exploiting and sharing cyber threat information.
- Extensive knowledge of how cyber-attacks unfold, from initial compromise to full execution, and how they can be prevented, detected, and responded to.
- Significant experience in coordinating the response to cyber incidents across large organization.
- Proven experience and success in leading a team and coordinating with multiple stakeholders to achieve the objective in adverse conditions.
- Experience in assessing vulnerabilities and their exploitation path and potential impact.
- Relevant experience in delivering and planning for operational cyber security services.
- Experience producing clear and concise presentations and reports to both technical and non-technical audiences as well as giving effective presentation.
- Excellent analytical, problem solving, and verbal and written communication skills.
- Business management experience in delivering IT services with a focus on continuous service improvement.
- Good understanding of the management of IT Service Delivery, following ITIL framework.
- Experience working on complex projects and coordinating multiple stakeholders in separate locations.

Education, Experience and Training (desirable):

Experience:

- Experience in proactive security measures such as compromise assessment, and adversary emulation to enhance the organization’s cyber resilience.
- NATO experience in the Cyber security field and understanding of new NATO’s organisation, including NATO Command and Force structure.
- Knowledge of potential security event sources and their interpretation and analysis in support of the incident detection and handling processes.
- Good knowledge and understanding of the monitoring, detection and automation technologies (e.g. SIEM, EDR, SOAR, FPC).

Training/Certifications:

- Cybersecurity certifications such as CISSP, CCSP, CISM or equivalent post-graduate degree in cybersecurity.
- Relevant certifications: GIAC Cyber Incident Leader, GIAC SOC Manager, ITIL or equivalent.

Behavioural competencies:

- Leading and Managing. Provides others with a clear direction; motivates and empowers others; inspires and drive cross-functional teams; attracts and develops staff of a high calibre; provides staff with development opportunities and coaching; sets appropriate standards of behaviour.
- Planning and Organising. Sets clearly defined objectives; plans activities and projects well in advance and takes account of possible changing circumstances; identifies and organises resources needed to accomplish tasks; manages time effectively; monitors performance against deadlines and milestones.
- Coping with Pressures and Setbacks. Maintains a positive outlook at work; works productively in a pressurised environment; keeps emotions under control during difficult situations; handles criticism well and learns from it; balances the demands of a work life and a personal life.
- 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.

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.