JOB DESCRIPTION

Post Details:			
Post Title:	**Principal Cyber Security Infrastructure Specialist**	Organisational Element:	NCSC
		Job Family:	NCIA-Cyber Security Engineering
Rank/Grade:	G20		
Military/Civilian:	Civilian	Location:	Mons (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:

The Principal Cyber Security Infrastructure Specialist / Red Team Technical Lead is responsible for leading the design, development, and operation of red team infrastructure and R&D capabilities in direct support of red team operations. This role provides technical direction and hands-on leadership to infrastructure and research teams, ensuring tools, platforms, and environments are resilient, scalable, and aligned with operational objectives.

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.

Risk management:

- Carries out risk management activities within a specific function, technical area or project of medium complexity.
- Identifies risks and vulnerabilities, assesses their impact and probability, develops mitigation strategies and reports to the business.
- Involves specialists and domain experts as necessary.

Technology service management:

- Identifies and manages resources needed for budgeting, estimating, planning, developing and delivering a specified portfolio of technology services and systems.
- Engages with and influences stakeholders to ensure that services are developed and managed to meet agreed service levels, security requirements and other quality standards.
- Plans and manages the implementation of processes and procedures, tools and techniques for monitoring and managing the performance of technology services.
- Aligns the contribution of specified systems and services to clearly stated organisational and financial goals and performance targets.
- Recommends options for sourcing — whether in-house, outsourced, or a combination.
- Monitors performance of delivery teams and takes corrective action where necessary and in line with policies.

Incident management:

- Ensures that incidents are handled according to agreed procedures.
- Prioritises and diagnoses incidents.
- Investigates causes of incidents and seeks resolution.
- Escalates unresolved incidents.
- Facilitates recovery, following resolution of incidents.
- Documents and closes resolved incidents.
- Contributes to testing and improving incident management procedures.

Additional duties for this post:

Red team AI engineering:

- Leads and coordinates the design, development, and operation of red team infrastructure and R&D capabilities in direct support of red team operations.
- Collaborates with Red Team Operator Leads to tailor infrastructure and tooling to mission needs.
- Ensures operational security for the deployed infrastructure.
- Manages Red Team research and development activities with the goal of developing and utilizing automation, custom tools, scripts, and malware to replicate sophisticated cyber threats and evade detection mechanisms.
- Advises and mentors team members, and continuously evolves capabilities to reflect real-world threat actors and emerging technologies.
- Maintains documentation and secure configurations for repeatable operations.

Deputize for higher grade staff if required

Perform other duties as may be required

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:

- At least 5 years practical experience working in cybersecurity field (Security analyst/engineer, vulnerability researcher, penetration testing, red teaming, security architect).
- In-depth knowledge of adversary emulation, red teaming and purple teaming.
- Understanding of tactics, techniques and procedures of threat actors based on MITRE ATT&CK Framework.
- Understanding of the various types of detections available (defence in depth) and how to bypass them.
- Ability to create and use custom tools to automate and optimize red team engagements.
- Technical knowledge in system and network security, authentication and security protocols, cryptography and application security.
- Proven experience leading interdisciplinary teams, preferably in international environment.
- Knowledge of vulnerability assessment and penetration testing methodologies.
- Proficiency in Red team tools and technologies.
- Knowledge of the latest security trends and best practices.
- Excellent communication and negotiation skills across technical, non-technical and Executive audiences.
- Strong analytical and problem-solving skills, with the ability to make data-driven decisions.

Training/Certifications:

- Cybersecurity oriented certification such as CRTP, GPEN, GWAPT, OSCP, OSCE, OSEE, GXPN, Red

team operator related certification, GREM.

Education, Experience and Training (desirable):

Experience:

- Knowledge of low-level programming languages (i.e Assembly, ARM).
- Advanced knowledge in C, C++.
- Experience in malware development / malware analysis.
- Experience in reverse engineering.
- Experience in C2 infrastructure management (redirectors / CDN / beaconing techniques).
- Experience in Infrastructure as Code (IaC) using tools like Terraform, Ansible, etc. to deploy and manage IT infrastructure.
- Advanced knowledge of Active Directory Services.
- Proven hands-on experience in penetration testing and adversary emulation.
- Proven experience in Blue/Red or purple teaming assessments.
- Expert knowledge of people management practices and principles.
- Knowledge of NATO or national governmental acquisition policy and procurement procedures.
- Prior experience of working in an international environment comprising both military and civilian elements.
- Knowledge of NATO responsibilities and organization, including Allied Command Operations and Allied Command Transformation.

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.
- *Leading and Managing* - Provides others with a clear direction ; motivates and empowers others; attracts and develops staff of a high calibre ; provides staff with development opportunities and coaching; sets appropriate standards of behaviour.

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.
Travel:	- Business travel to NATO and national (NATO and non-NATO) facilities as well as frequent travel between the NCIA offices; - May be required to undertake duty travel to operational theatres inside and outside NATO boundaries.

Work Environment:	Normal office environment.