JOB DESCRIPTION

Post Details:			
Post Title:	**Principal Cyber Security Assessor**	Organisational Element:	NCSC
		Job Family:	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:

A Principal Cyber Security Assessor is responsible for evaluating and testing of an organization's information systems to identify vulnerabilities and potential security threats. They oversee the conduction of comprehensive security assessments, analyze security data, and develop recommendations to improve the organization's overall security posture. They perform risk assessments, analyze security policies and procedures, and recommend security enhancements to protect against cyber-attacks. They provide guidance and support to other members of the security team and may be responsible for managing and overseeing junior assessors.

Under the direction of the Red Team Leader, the Principal Red Team Operator conducts covert security assessments by planning and executing sophisticated cyberattacks to rigorously assess and improve NATO's defences.

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.

Vulnerability research:

- Plans and manages vulnerability research activities.
- Maintains a strong external network in the area of vulnerability research.
- Gathers information on new and emerging threats and vulnerabilities.
- Assesses and documents the impacts and threats to the organisation.
- Creates reports and shares knowledge and insights with stakeholders.
- Providing expert advice and guidance to support the adoption of tools and techniques for vulnerability research.
- Contributes to the development of organisational policies, standards, and guidelines for vulnerability research and assessment.

Specialist advice:

- Provides organisational leadership and guidelines to promote the development and exploitation of specialist knowledge in the organisation.
- Maintains a network of recognised experts (inside and/or outside the organisation) who can deliver expert advice in relevant areas.
- Provides input into professional development planning across a significant part of the organisation to further the development of appropriate expertise.

IT infrastructure:

- Provides technical leadership to optimise the performance of IT infrastructure.
- Investigates and manages the adoption of tools, techniques and processes (including automation) for the management of systems and services.
- Oversees the planning, installation, maintenance and acceptance of new and updated infrastructure components and infrastructure-based services.

- Aligns to service expectations, security requirements and other quality standards.
- Ensures that operational procedures and documentation are fit for purpose and kept up to date.
- Ensures that operational issues are identified, recorded, monitored and resolved.
- Provides appropriate status and other reports to specialists, users and managers.

Vulnerability assessment:

- Plans and manages vulnerability assessment activities within the organisation.
- Evaluates and selects, reviews vulnerability assessment tools and techniques.
- Provides expert advice and guidance to support the adoption of agreed approaches.
- Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems.

Additional duties for this post:

Red team Operations:

- Participates to the planning, design, and execution of red team engagements that simulate adversarial tactics, techniques and procedures against enterprise systems, covering network, applications and cloud domains.
- Conducts reconnaissance, open-source intelligence (OSINT) gathering, vulnerability scanning, exploitation, lateral movement, persistence installation, and command & control management during offensive security operations.
- Performs research and development activities with the goal of developing and utilizing custom tools, scripts, and malware to replicate sophisticated cyber threats and evade detection mechanisms.
- Performs social engineering and phishing campaigns to assess the effectiveness of human and process defences.
- Creates clear and actionable reports for both technical teams and executive stakeholders.

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 offensive cybersecurity field (vulnerability researcher, penetration testing, red teaming).
- Extensive knowledge and experience (at least 5 years) in the following areas:
    - Conducting or leading Red Team engagements;
    - Web application penetration testing;
    - IT infrastructure penetration testing;
    - Network security architecture design;
    - Assessing security vulnerabilities within OS, software, protocols & networks;
    - Researching and evaluating security products & technologies;
    - Knowledge in system and network administration of UNIX and Windows systems;
    - Use of penetration testing tools, techniques, and recognized testing methodologies;
    - Scripting skills in at least one of the following: Perl, Python, Ruby, shell (bash, sh).
- Practical experience identifying vulnerabilities and discovering 0days.
- Understanding of the principles of adversary emulation.

- Understanding of tactics, techniques and procedures of threat actors based on MITRE ATT&CK Framework.
- Ability to create and execute custom scripts to simulate attack activities.
- Understanding of the various types of detections available (defence in depth) and how to bypass it.
- Knowledge of the latest security trends and best practices.
- Ability to create and use custom tools to automate and optimize red team engagements.
- Experience with security testing tools and methodologies, such as fuzzing, static and dynamic application security testing, and penetration testing.
- Use of red teaming tools, techniques, and recognized testing methodologies.
- Technical knowledge in system and network security, authentication and security protocols, cryptography and application security.
- Proven ability to write clear and structured technical reports including executive summary, technical findings and remediation plan for several different audiences.

Training/Certifications:

- Cybersecurity oriented certification such as GRTP, GPEN, GWAPT, OSCP, OSCE, OSEE, GXPN, Red team operator related certification, GREM.

Education, Experience and Training (desirable):

Experience:

- CVE attribution/recognition following a responsible disclosure of a 0day.
- Knowledge of low-level programming languages (i.e Assembly, ARM).
- Advanced knowledge in C, C++.
- Experience in malware development.
- Experience in reverse engineering.
- Experience in C2 infrastructure management (redirectors / CDN / beaconing techniques).
- Advanced knowledge of Active Directory Services.
- Knowledge of at least one big cloud provider: Azure, Amazon AWS, GCP.

Behavioural competencies:

- *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.
- *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.