JOB DESCRIPTION

Post Details:			
Post Title:	**Senior Cyber Security Assessor**	Organisational Element:	NCSC
		Job Family:	Cyber Security Engineering
Rank/Grade:	G17		
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 Senior Cyber Security Assessor is responsible for evaluating and testing an organization's information systems to identify vulnerabilities and potential security threats. They conduct 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 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 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.

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.

Vulnerability research:

- Designs and executes complex vulnerability research activities.
- Specifies requirements for environment, data, resources and tools to perform assessments.
- Reviews test results and modifies tests if necessary.
- Creates reports to communicate methodology, findings and conclusions.
- Makes an active contribution to research communities.

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.
- Supports and promotes the development and sharing of specialist knowledge within the organisation.

IT infrastructure:

- Provides technical expertise to enable the correct application of operational procedures.
- Configures tools and/or creates scripts to automate the provisioning, testing and deployment of new and changed infrastructure.
- Investigates and enables the resolution of operational issues.
- Provides reports and proposals for improvement, to specialists, users and managers.

Vulnerability assessment:

- Collates and analyses catalogues of information and technology assets for vulnerability assessment.
- Performs vulnerability assessments and business impact analysis for medium complexity information systems.
- Contributes to selection and deployment of vulnerability assessment tools and techniques.

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 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 NCIA, that is, at least 10 years extensive and progressive expertise in duties related to the function of the post.

Experience:

- At least 3 years practical experience working in cybersecurity or a related field, such as information technology, network administration, or software development.
- Extensive knowledge and experience (at least 3 years) in the following areas:
    - 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)
- Relevant practical experience identifying vulnerabilities and discovering potential 0days.
- Proven experience in penetration testing, adversary emulation or Red teaming for at least 3 years.
- 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 penetration testing 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 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.
- 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.