JOB DESCRIPTION

Post Details:			
Post Title:	**Cyber Security Assessor**	Organisational Element:	NCSC
		Job Family:	Cyber Security Engineering
Rank/Grade:	G15		
Military/Civilian:	CIV	Location:	Mons, BEL

Organization 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:

A Cyber Security Assessor is responsible for evaluating and testing an organization's information systems to identify vulnerabilities and potential security threats. They conduct risk assessments, analyse security policies and procedures, and recommend security enhancements to protect against cyber-attacks. They also provide guidance and training to employees on best practices for information security.

Duties and Responsibilities:

Information security:

- Communicates security risks and issues to business managers and others.
- Performs basic risk assessments for small information systems.
- Contributes to the identification of risks that arise from potential technical solution architectures.
- Suggests alternate solutions or countermeasures to mitigate risks.
- Occasionally prepare, maintain and manage Security Hardening, Configuration and Installation guidelines. Mostly, but not limited to the following areas:
    - Public Cloud Infrastructure Services;
    - Container security;
    - Network Infrastructure Security;
    - Web Servers.
- Supports investigation of suspected attacks and security breaches.

Information assurance:

- Follows standard approaches for the technical assessment of information systems against information assurance policies and business objectives.
- Recognises decisions that are beyond their scope and responsibility level and escalates according.
- Reviews and performs risk assessments and risk treatment plans.
- Identifies typical risk indicators and explains prevention measures.

Vulnerability Management:

- Execute Vulnerability Management duties, based on the Security findings reported from the assessment campaigns. This includes:
    - Validating the severity of discovered vulnerabilities;
    - Contextualising the vulnerabilities in the light of NATO policies and best practices;
    - Determining possible remediation and mitigation measures;
    - Defining / Assigning priorities;
    - Contacting and liaising with relevant system owners and proposing a remediation plan;
    - Track and trace all remediation actions and report to the relevant stakeholders.
- Collect and consolidate the vulnerabilities discovered with the assessment services.
- Support NCI Agency CIS Support Units and other NATO entities and customers in the process of vulnerability remediation.
- Compile, draft, review, develop, and provide input on all relevant aspects relating to vulnerability management and mitigation process in NATO CIS.
- Brief at both executive and technical levels on Vulnerability Management reports and mitigations status, including at flag officer level.

Specialist advice:

- Provide CIS Security related input to NATO Directives in the Cyber Security area.
- Provide security consultancy and advice to projects, plans and teams.
- Reviews documents to be published on NCSC Portals, or provided to NCSC customers, as part of projects deliverables.
- Provide CIS Security related input to NATO Directives in the Cyber Security area.

- Ensures links and maintains relationships with major vendors in order to have opportunity to influence development of security guidance leading to shorter implementation timelines.

Additional duties for this post: This position is specifically employed in the area of Vulnerability Mitigation.

Vulnerability Assessor	VUAS	Vulnerability Assessment
Systems Security Analyst	SCAD	Security Operations
Vulnerability Manager	VURE	Vulnerability Research

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:

At least 2 years practical experience working in cybersecurity or a related field, such as information technology, network administration, or software development.

Extensive knowledge of Cloud System Security Services and Configuration.

Experience in modern CIS secure deployment and configuration troubleshooting.

Extensive experience in the contextual interpretation of Vulnerability Assessments results.

Comprehensive understanding of the principles of computer and communications security, networking, and the vulnerabilities of modern operating systems and applications acquired through a blend of academic or professional training coupled with practical professional experience.

Proven, professional experience and expert knowledge in at least three of the following:

- Implementation and integration of Information Assurance protective measures;
- Security mechanisms related to modern Web Application Security;
- Security mechanisms and administration of LAN and WAN in the large enterprise environment;
- Private and public cloud security;
- Enterprise system administration experience of Windows Active Directory concepts and architecture.
- Light virtualisation/container security concepts;
- Enterprise system administration experience of VMWare vSphere environment and architecture, with emphasis on security concepts design and implementation.

Excellent communication skills with respect to briefing/presenting, report writing & mediation.

Proven ability to write clear and structured technical reports including executive summary, technical findings and remediation plan for several different audiences.

Training/Certifications:

Industry leading certification in the area of Cyber Security such as SANS GIAC certifications in the 400/500 or 600 series, ISC2 CISSP and ITIL Foundation.

Education, Experience and Training (desirable):

Experience:

Experience in secure evaluation and/or accreditation of communications and information systems.

Experience in data processing automation using script languages (e.g. PowerShell/PowerCLI, Python, Bash etc.).
Prior experience of working in an international environment comprising both military and civilian elements.

Knowledge of NATO responsibilities and organization, including ACO and ACT.

Training/Certifications:

Recognized professional training/qualification within the Vulnerability Auditing field of expertise.

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.
- Adhering to Principles and Values - Upholds ethics and values; demonstrates integrity; promotes and defends equal opportunities, builds diverse teams; encourages organisational and individual responsibility towards the community and the environment.
- 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.
- Achieving Personal Work Goals and Objectives: Accepts and tackles demanding goals with enthusiasm; works hard and puts in longer hours when it is necessary; seeks progression to roles of increased responsibility and influence; identifies own development needs and makes use of developmental or training opportunities.

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.