JOB DESCRIPTION

Post Details:			
Post Title:	**Senior Engineer (Crypto Validation)**	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 Infrastructure Specialist is responsible for designing, implementing, and maintaining an organization's security infrastructure. They identify potential security vulnerabilities and develop strategies to mitigate them. They also monitor and analyze security systems to detect and respond to security incidents. This role requires expertise in network security, firewalls, intrusion detection and prevention systems, and other security technologies. He/she consults with stakeholders to evaluate functional requirements and translate functional requirements into technical solutions.

Duties and Responsibilities:

Information security:

- Applies and maintains specific security controls as required by organisational policy and local risk assessments.
- 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.
- Defines secure systems configurations in compliance with intended architectures.
- 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.
- Makes routine accreditation decisions.
- 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.
- Maintains integrity of records to support and justify decisions.

Risk management:

- Undertakes basic risk management activities.
- Maintains documentation of risks, threats, vulnerabilities and mitigation actions.

Incident management:

- Provides first level investigation and gathers information to enable incident resolution and allocate incidents.
- Advises relevant persons of actions taken.

Additional duties for this post:

Under the direction of Crypto Capability Validation Team lead but working largely on their own initiative, the incumbent will perform additional duties such as:

General Responsibilities:

- Supporting the vision and mission of the NCSC and ensuring Branch technical adherence to broader

Business Area initiatives.
- Engage with and provide support to NCSC's Transform Branch in its Solution Architecture activities in the area of Crypto.
- Collaborate closely with Service Transition and Continuous Service Improvements cross functional activities.

Information Security:

- Provides advice and guidance to security solutions to manage identified risks and ensure adaptation and adherence to standards.
- Identifies risks that arise from potential technical solution architectures.

User Experience Analysis:

- Identifies the roles of affected stakeholders.
- Resolves potential conflicts between differing user requirements.

Emerging Technology Monitoring:

- Monitors the external environment to gather intelligence on emerging technologies.

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 of designing, implementing, and maintaining security infrastructure.
- Practical experience identifying and mitigating security vulnerabilities.
- Extensive expertise in network security, firewalls, intrusion detection and prevention systems.
- Experience in the development of technical requirements, system diagrams and other engineering products to aid cybersecurity procurements and support.
- Proven ability to deliver security capabilities to industry, government or military.
- Recognised track record in dealing with stakeholders, understanding their needs, problems and requests and proposing constructive courses of action.
- Proven experience in IT security consulting or in a similar role with demonstratable track record of delivering sizeable and complex IT security projects.
- Proven experience designing and implementing security on major cloud platforms or enterprise networks.
- Proven experience creating, testing, and implementing secure infrastructures.
- Proven ability and desire to stay up to date with the latest security technologies and trends.
- Proven ability to communicate effectively, orally and in writing with good presentation skills.

Education, Experience and Training (desirable):

Experience:

- Prior experience working in an international environment comprising both military and civilian elements.
- Knowledge of NATO responsibilities and organization including ACO and ACT.

Training/Certifications:

- Relevant certifications in cyber security such as Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP) or Global Information Assurance Certification (GIAC).
- Relevant certification in ITIL Service Management.

Behavioral 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.
- *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.
- *Adapting and Responding to Change* - Adapts to changing circumstances; tolerates ambiguity; accepts new ideas and change initiatives; adapts interpersonal style to suit different people or situations; shows an interest in new experiences.

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 between the NCIA offices. May be required to undertake duty travel to operational theatres inside and outside NATO boundaries
Work Environment:	Normal office environment with ad hoc work in technical workshop.