JOB DESCRIPTION

Post Details:

Post Title:	**Senior Cyber Security Engineer**	Organisational Element:	COO/NCSC
Military/Civilian:	CIV	Location:	Mons/BEL

Organisation 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 Business Areas, Programme Offices, CIS Support Units/Elements, and the Agency Ops Centre. The NCSC is responsible for providing the breadth 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.

The Capability Development (CD) Branch ensures that cyber security is properly addressed during the planning, design and implementation of CIS services and capabilities ensuring a coherent and effective cyber security architecture across all NCI Agency CISs. The required security services and capabilities are provided and managed throughout the CIS lifecycle to meet the cyber security expectations of the customer as well as the requirements of the NATO security policies and supporting directives. The CD Branch also provides lifecycle Security Risk management support to all NATO CIS, long term planning input for evolving CS services, support to the architectural development within the Agency as well as technical and policy support to the NATO Security Accreditation Authorities. Finally, the CD Branch leads cyber innovation services that, by enabling the structured development of creative and innovative new security solutions, are a key element of NATO's transformation in the area of cyber security.

Job role description:

As a Senior Cyber Security Engineer, the primary responsibility will be to develop effective, agile and resilient cyber security solutions tailored to specific operational requirements and environmental conditions. He/she consults with stakeholders to evaluate functional requirements and translate functional requirements into technical solutions. They design, develop, test, and evaluate information system security throughout the systems development life cycle and are responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.

Duties and Responsibilities:

Solution architecture:

- Contributes to the development of solution architectures in specific business, infrastructure or functional areas.
- Identifies and evaluates alternative architectures and the trade-offs in cost, performance and scalability.
- Determines and documents architecturally significant decisions.
- Produces specifications of cloud-based or on-premises components, tiers and interfaces, for translation into detailed designs using selected services and products.
- Supports projects or change initiatives through the preparation of technical plans and application of design principles.
- Aligns solutions with enterprise and solution architecture standards (including security).

Cyber 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.

Requirements definition and management:

- Defines and manages scoping, requirements definition and prioritisation activities for initiatives of medium size and complexity.
- Contributes to selecting the requirements approach.
- Facilitates input from stakeholders, provides constructive challenge and enables effective prioritisation of requirements.
- Establishes requirements baselines, obtains formal agreement to requirements, and ensures traceability to source.

User experience analysis:

- Selects appropriate techniques and tools to develop user stories and elicit user experience requirements in complex situations.
- Identifies and describes the design goals for systems, products, services and devices.

- Identifies the roles of affected stakeholder groups.
- Resolves potential conflicts between differing user requirements.
- Specifies measurable criteria for the required usability and accessibility of systems, products, services and devices.

Additional duties for this post:

Under the direction of the Solutions and Roadmaps Section Head and in consultation with NCSC Service Owners, but largely on their own initiative, the incumbent will perform duties such as the following:

General responsibilities:

- Supporting the vision and mission of the NCSC and ensuring NCSC technical adherence to broader NCIA initiatives under the direction and guidance of the NCSC Solutions Roadmap Section Head (Cyber).
- Working in consultation with NCSC Service Owners on evolution of NCSC services and developing Cybersecurity Service Roadmaps.
- Supports development of architectural directives and architecture products; working hand in hand with the NCSC lead for design and implementation.
- Provides support to staff working on projects where Cyber Security is being evolved, uplifted or transformed.
- Represent the NCIA/ NCSC in working groups and forums.
- Ensure awareness and anticipates potential business changes to be able to predict impact on capability and technology challenges; working hand in hand with the NCSC lead for research, policy and innovation.
- Support policy and directive updates (NATO and NCI Agency) / changes, assess potential impact on capabilities and service, propose changes and updates, draft and contribute to relevant policy.
- Deputizes for higher-grade staff, if required.
- Performs any 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 developing or delivering services in Cybersecurity.
- Extensive practical experience identifying vulnerabilities and potential security threats.
- Development of technical requirements, system diagrams and other engineering products to aid Cybersecurity acquisition and procurement.
- Proven ability to deliver cyber security capabilities for industry, government, or military.
- Up to date knowledge and experience in the following areas:

- ✓ Design and implementation of cyber security capabilities and supporting infrastructure elements in an operational environment;
- ✓ Cryptographic technologies including key management;
- ✓ Identity and access management;
- ✓ Risk management.

- Knowledge in the following areas:
  - ✓ Network monitoring and detection technologies;
  - ✓ The design of cyber security capabilities on cloud infrastructure.
- Ability to apply architecture methodologies to express complex, systems of systems in architectural terms and models of varying detail; Recognised track record in dealing with stakeholders, understanding their needs, problems, and requests and proposing constructive ways ahead.
- Proactive attitude in seeking and maintaining trust from stakeholders.
- Proven ability to communicate effectively orally and in writing with good briefing skills.
- Very good communication and analytical skills.
- Experience leading small teams.

Education, Experience and Training (desirable):

Experience:

- 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:

- Relevant certifications, such as Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP) or GIAC Security.

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 NCI Agency is conducted in the English language.