JOB DESCRIPTION

Post Details:

Post Title:	**Cyber Security Engineer**	Organisational Element:	NCSC
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:

As a Cybersecurity Engineer, you will be responsible for engineering, integrating, and maintaining secure, resilient, and mission-critical cybersecurity solutions that meet operational, technical, and security

requirements. The role provides specialist technical expertise across enterprise security architecture, Microsoft infrastructure technologies, identity and access management, secure application and web platforms, database services, and system integration.
You will work closely with technical and operational stakeholders to translate functional and security requirements into robust and maintainable solutions. Operating across the full system lifecycle, you will contribute to solution design, security engineering, integration, testing and validation, transition into operation, troubleshooting, continuous improvement, and lifecycle management, ensuring solutions remain secure, reliable, and aligned with operational needs and applicable security standards.

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).

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.

Requirements definition and management:

- Defines and manages scoping, requirements definition and prioritisation activities for small-scale changes and assists with more complex change initiatives.
- Follows agreed standards and applies appropriate techniques to elicit and document detailed requirements.

- Provides constructive challenge to stakeholders as required.
- Reviews requirements for errors and omissions.
- Prioritises requirements and documents traceability to source.
- Provides input to the requirements base-line.
- Investigates, manages and applies authorised requests for changes to base-lined requirements, in line with change management policy.

User experience analysis:

- Applies standard techniques and tools for developing user stories and eliciting user experience requirements.
- Organises and structures user experience analysis.
- Works with stakeholders to prioritise requirements and resolve conflicts.

Additional duties for this post:

Under the direction of the DICE Team Lead and in coordination with the SEC036 Service Delivery Manager, you will act as a Senior Microsoft Technologies Subject Matter Expert, with primary responsibility for the full technical lifecycle management of dedicated NCSC Web Access Layer infrastructure components. This includes, but is not limited to:

- Microsoft SharePoint farms, including configuration, maintenance, patching, troubleshooting, service application management, authentication integration, and performance tuning.
- Web Application Proxy and AD FS federation nodes, including federation trust configuration, claims-based authentication, certificate lifecycle management, Single Sign-On strategy, and secure access publishing.
- DMZ-based publishing and reverse proxy/load-balancing components, including high-availability configuration, secure routing, TLS/SSL inspection considerations, health monitoring, and service publication.
- SQL Server Always On availability groups and associated endpoints and databases, including database availability, replication, backup and recovery support, connectivity troubleshooting, and dependency management.
- NCSC Replicator System components and related data exchange or synchronisation mechanisms supporting web access and publication services.
- You will perform advanced day-to-day administration, preventive maintenance, technical troubleshooting, configuration management, and operational support for these platforms. The role requires the ability to diagnose complex incidents across multiple technical layers, including identity and access management, web publishing, network connectivity, certificates, DNS, load balancing, database back-end services, application dependencies, and security monitoring integrations.
- You will also participate in project activities affecting the supported infrastructure, providing technical assessment, design input, implementation support, testing, migration planning, and operational acceptance. In addition, you will support the internal NCSC D-CAB change management process by preparing technical change documentation, assessing implementation risks, defining rollback procedures, supporting change execution, and validating post-change service stability.
- When required, you will assist the SEC036 Service Delivery Manager with the upgrade, maintenance, and technical support of specialised SharePoint portals and custom web portals, with particular focus on the NIAPC — NATO Information Assurance Product Catalogue — web portal hosted within the NCIA AWS Cloud Environment. This may include support to application hosting, authentication integration, secure publishing, platform upgrades, cloud-hosted service dependencies, availability monitoring, and coordination with relevant infrastructure and security teams.

- You will be responsible for maintaining accurate technical and operational documentation, including system configuration records, design notes, change records, operational procedures, troubleshooting guides, task tracking and project documentation using platforms such as JIRA and Confluence.
- The role will also support service management and reporting activities, including automated KPI evaluation, with particular emphasis on availability, service health, web publication status, and operational performance of the maintained frameworks. You will contribute to the development and maintenance of monitoring, alerting and reporting mechanisms required to ensure service reliability and measurable operational effectiveness.
- Where required, you will ensure the correct technical integration of the systems under management with related NCSC frameworks and security services, including NPKI, ACPV, CDSA, SIEM, and OVA. This includes validating interface dependencies, authentication and certificate requirements, event forwarding, logging, monitoring, vulnerability management, and secure interoperability across the supported service layers.

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 NCIA, that is, at least 6 years extensive and progressive expertise in duties related to the function of the post.

Experience:

- Strong knowledge and experience in designing, installing and managing complex and modern Microsoft SharePoint environment for at least 500 end-users.
- Strong knowledge and demonstrable experience with web development technologies including ASP.NET, JavaScript and the use of REST API.
- Strong experience in user-focused development approach and working in an agile project management framework.
- Strong experience with Identity and Access Management (IDAM) & SSO Federation technologies (AD FS / Keycloak) and protocols (SAML / OIDC).
- Strong team-spirit attitude.
- Good Knowledge and experience using Microsoft SCCM / SQL Server / Exchange.
- Experience in developing custom SharePoint solutions using .NET Webforms (custom features, timer jobs, webparts, custom actions).
- Have an in-depth understanding of infrastructure concepts related to Hosting, Networks, IP address Management, firewalls, certificates, Load balancing and Proxy.
- Knowledge and demonstrable experience with scripting languages and integration tools including PowerShell, Python and SQL.
- Good understanding of cyber security concepts.
- Good understanding of network communication protocols.
- Working experience with SecDevOps within cloud environments such as Azure, AWS, GCP.
- Good working knowledge of version control systems such as GIT.

Education, Experience and Training (desirable):

- Experience developing .NET desktop applications (WPF, MVVM, Windows Background Service, Dependency Injection, Entity Framework 6, Serilog, xUnit, Moq, Azure DevOps).
- Working experience in the cyber security area.
- Past experience working for NATO.
- Strong cyber security skills.

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.
- *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 NCIA is conducted in the English language.