JOB DESCRIPTION

Post Details:			
Post Title:	**Senior Technician (Cyber Security Infrastructure)**	Organisational Element:	NCSC
Military/Civilian:	Civilian	Location:	Mons, Belgium (BE)

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) 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:

The role is responsible for providing advanced technical support for enterprise endpoint security solutions (such as anti-malware, Data Loss Prevention, application whitelisting, disk wiping and data encryption), managing their full lifecycle from testing and deployment to maintenance, and ensuring they are securely

configured and documented. It also involves monitoring the evolving cyber threat landscape, responding to security incidents and vulnerabilities, maintaining the security and resilience of enterprise systems, supporting compliance with security policies, and providing technical expertise to improve overall cybersecurity operations.

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.

IT infrastructure:

- Carries out routine operational procedures, including the execution of specified automation tools/scripts.
- Amends existing automation tasks under supervision to gain a basic understanding of the scripting language/automation tools.
- Contributes to maintenance and installation.
- Monitors and reports on infrastructure performance to enable service delivery.
- Resolves issues or refers to others for assistance.

Incident management:

- Follows agreed procedures to identify, register and categorise incidents.
- Gathers information to enable incident resolution and allocates incidents as appropriate.

Additional duties for this post:

- Provides NATO-wide support on endpoint protection solution, such as anti-malware, removable device control, Data Loss Prevention, application whitelisting, disk wiping and Hard-Drive encryption solutions.

- Follows the software life cycle management (such as release, testing, distribution and maintenance) of a variety of enterprise endpoint protection tools.
- Develops and tests the settings, and produces installation and configuration guidelines.
- Monitors the IT security threat landscape (mainly malware trends) and emerging security protection products.
- Communicates security risks and issues to business managers and others.
- 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.
- Maintains integrity of records to support and justify decisions.
- Reviews, tests and installs appropriate firmware, security patches and upgrades for all Microsoft-based services and windows-based operating systems at various locations and enclaves.
- Provides remediation plans for the testing and implementation of third-party firmware and security patches on infrastructure servers and client workstations.
- Provides general technical support to the platform and infrastructure services to resolve end user issues.
- Conducts performance testing and tuning on host and operating systems.
- Supports NCSC service desk on related service requests, incidents and problems.
- Troubleshoots, diagnoses and resolves the incidents and problems onsite or remotely.
- Supports NCSC change management activities as SME and implementers when required, configures and manages Microsoft OS and client application patching for both servers and workstations.
- Performs any other duties as may be required.

Education, Experience and Training (essential):

Education:

- Higher vocational training in a relevant discipline with 2 years post-related experience. Or a secondary educational qualification with 4 years post-related experience.

Experience:

- At least 2 years practical experience of implementing and maintaining security infrastructure.
- At least 2 years of experience in managing and supporting COTS endpoint protection solutions from security vendors such as Trellix/McAfee, Symantec, Trend Micro, Sophos, etc.
- At least 2 years of experience in malware protection technologies, malicious code techniques and associated countermeasures.
- At least 2 years of experience in managing and supporting other endpoint security solutions such as application whitelisting, host intrusion prevention, secure erasure, data loss prevention, drive encryption, disk wiping etc.
- At least 2 years of experience in software selection, evaluation and benchmarking.
- Experience in vendor relationship management including support account management and licence management.
- Experience in the implementation and integration of Cyber Security protective measures.
- Excellent communications skills and reporting experience with capacity to communicate to different types of audience (senior executive, middle management, technical and non-technical).

- Direct system administration experience with Linux, Windows Server and Windows 11 operating system environments.
- Good experience with Microsoft Active Directory, account lifecycle management, creating/supporting of group policy objects and organizational units.
- Fundamental knowledge of administering of MS SQL servers.
- Strong understanding of security issues surrounding server OS and applications.
- Fundamental understanding of storage area networks (SAN) concepts, protocols and technologies related to FC, iSCSI, WWN, soft/hard zoning, RAID protection levels, LUN masking, IOPS, read/write latency, deduplication, data clone/snapshot/replication.
- Fundamental understanding of backup and restore related concepts and technologies (i.e. full/differential/incremental backups, VM-based backups, application-aware backups, single item recovery, virtual/physical tape drives).
- Fundamental understanding of multi-factor authentication (MFA) concepts and technologies.
- Fundamental understanding of infrastructure concepts related to Hosting, Networks, IP Address Management, firewalls, certificates, Load balancing and Proxy.
- Good understanding on internet protocols including HTTP, SSL, TCP, IP.

Education, Experience and Training (desirable):

Training/Certifications:

- Microsoft MCSA/MCSE or equivalent certification.
- Professional certifications such as from; ISC2, ISACA, GIAC, or other recognized certification programmes, ideally with emphasis on IT security.

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.
- *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 NCI Agency is conducted in the English language.
Work Environment:	The work is normally performed in a typical Secure Facility environment.
Supervises:	The incumbent may give professional guidance to staff.
Professional Contacts:	Coordination and cooperation of work with activities in other Service Lines within

the NCIA