Duty Location: **Naples, ITA**

JOB DESCRIPTION

Senior Technician (Cyber Security Operations)

Directorate of CIS Support Units – CSU Naples

Grade: **G10**

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.

The Directorate of CIS Support Units (DCSU) is responsible to manage, deliver and maintain assigned Communications and Information System (CIS) products and services for the Agency's customers including NATO Headquarters (NHQ), the NATO Command Structure (NCS), NATO Force Structure (NFS), Nations and internal Agency users. DCSU provides liaison, planning and coordinating functions for Alliance Missions, Operations and Exercises. Services are delivered in coordination with the Enterprise Service Operations Centre (ESOC) and Agency Service Lines/Service Centres under the Enterprise Service Delivery Model (ESDM).

NCI Agency CIS Support Unit (CSU) Naples, located in Naples (ITA) enables end-to-end CIS services as it installs, operates, maintains and supports the full range of CIS capabilities during peacetime, crisis and war throughout its allocated Area of Responsibility (AOR) and as otherwise directed. One of the three main datacentres in NATO is hosted in Naples, resourced by the relevant Service Line and supported by the CSU.

The Service Operations Branch (SOB) is responsible for providing local support to the provision of CIS services in direct support of local and remote customers in accordance with SLAs and other agreements. SOB ensures physical Security is monitored and maintained, and Cyber Security activities are performed as delegated by NATO Cyber Security Centre (NCSC).

Under SOB AOR, Cyber Security Section (CSS) in conjunction with the NATO Cyber Security Centre (NCSC) contributes to the accreditation process, involving document preparation, Communication Security (COMSEC) and Computer Security (COMPUSEC) pre-inspections within the CSU AOR. CSS provides policy support, capability development, engineering and transitioning, security incident process as appropriate for the CSU AOR. CSS is responsible for assigned security application services and security management for assigned hardware. CSS contributes to Vulnerability Assessments, Incident Management, Problem Management, Level 1 and 2 support, IT Service Continuity Management, Supplier Management, Configuration Management and Change Management as appropriate within its area of expertise. CSS provides awareness briefings in accordance with the SLA.

Duties:

Under the direction of Cyber Security Section Head and CIS Security Officer, the incumbent will perform duties such as the following functions:

- Identifying system vulnerabilities and possible threats and then applying the necessary safeguards (both technical and administrative) to minimize those vulnerabilities and defend against potential attacks;
- Providing advice and assistance to various personnel (technical and non-technical) in identifying security requirements for the different automated systems including security considerations in application development, implementation, operation and maintenance;
- Supporting security awareness and training for site users;
- Maintaining close liaison with NCSC and cooperating with external security stakeholders on all computer-related security issues;
- Applying cyber security policies at the local level and as required;
- Providing technical expertise to install new network equipment;
- Providing technical advice to the CIS Security Officer in performing risk assessments, in resolving problems with security systems, and in implementing CIS infrastructures;
- Preparing technical documentation for accreditation processes and for COMSEC, EMSEC, TRANSEC inspections within the AoR, in support of the customer;
- Communicating security issues and concerns to management staff;
- Investigating security incidents and taking appropriate actions;
- Manage and monitor patch management on all systems; troubleshoot possible patch applications problems on workstations in close coordination with NCSC; and coordinate with TMS and AMS problems on servers;
- Deputize for higher grade staff, if required;
- Performs other duties as may be required.

Experience and Education:

- Higher vocational training in a relevant discipline (such as IT/ Cyber Security) with 2 years post-related experience. Or a secondary educational qualification with 4 years post-related experience, leading to a formal technical or professional certification;
- Extensive knowledge of the principles of CIS/Cyber Security, networking, of modern operating systems and applications, and their vulnerabilities;
- General knowledge of Crypto systems and technique;
- Extensive knowledge of Internet Protocol based networks and components (routers and switches).
- Experience in the analysis of risk and in the implementation and integration of Cyber Security protective measures;
- Satisfactory experience in using patch management systems, such as SCCM.
- Thorough expertise in McAfee ePO.

Desirable Experience and Education:

- Prior experience of working in an international environment comprising both military and civilian elements;
- Knowledge of NATO responsibilities and organization, including ACO and ACT;
- Experience with implementation projects within NATO and/or National military organizations;
- Knowledge of policy, procedures, and organisation of NATO CIS;
- Knowledge of NATO networks, security policies and directives;
- Working knowledge of ITIL processes and procedures;
- Experience in working in a service desk environment;
- Desirable Courses:
  - 0731 - Cyber Defence NATO COMPUSEC Level 1.
  - 0732 - Cyber Defence NATO COMPUSEC Level 2.

- 0280 - Cyber Defence NATO CIS Security Officer Version 2 (or NATO INFOSEC Officer Version 1).
- MCSE: Core Infrastructure.
- McAfee Certified Product Specialist.

Language Proficiency:

– 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.

Competencies or Personal Attributes:

– 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.

– 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.

– 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.