NOTIFICATION OF A VACANCY AT 1st NATO SIGNAL BATTALION

DUTY LOCATION: WESEL, Germany

JOB TITLE: Technician (Cyber Defence)

NATO International Civilian Grade: B-4

POST NUMBER: ODN MCMX 0050

DUE DATE for receipt of applications: 4 March 2020

Post Context:
NSB provides CIS services to deployed NATO HQs.
The Maintenance and Support Company is responsible for technical support of Command and Control services (including Information Systems Support to Functional Services), by providing electronic maintenance (level 2+) of deployable assets, for level 2 maintenance of Communications Information Systems (CIS) and Non-CIS equipment, and supply for the NATO Signal Battalion. The Communications and Information Systems Platoon is responsible for the operational planning and control of all level 2/2+ Communications Information Systems (CIS) maintenance assets in support of NATO operations and exercises.
The Mobile Communications and Information Systems and Cyber Defence Section is responsible for the level 2 electronic maintenance and cyber protection of Communications Information Systems equipment at all NATO locations. The incumbent is responsible for the protection of classified/unclassified NATO DCIS IS from vulnerabilities and threats.

Duties:
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 operation and maintenance.
Communicating security issues and concerns to management staff.
Investigating security incidents and, in conjunction with the NSB HQ S-2 and NATO CIS Group HQ, taking appropriate actions.
Maintaining close liaison with the NSB HQ S-2 and NATO CIS Group HQ on all computer-related security issues.
Supporting the provision of Cyber Defence services to operations and exercises.
Performing Level 2 vulnerability assessment, incident detection and response in the Deployable Network Operations Centre Cyber Defence Cell in support of NATO Operations and Exercises.
Assisting the NSB HQ S-2 in performing risk assessments and identifying potential security risks that may arise.
Developing, implementing and managing security awareness and training for supported users.
Assisting the resolution of technically challenging problems with the cyber defence services installed in the deployable networks and systems.
Travel requirements / contract:
The Technician (Cyber Defence) may be required to undertake deployments in support of military operations and exercises, and/or TDY (duty travel) assignments, both within and outside NATO boundaries. Such operational deployment may be up to a total 6 months (uninterrupted or in shorter periods) in any period of 18 months and may be on short notice.
Acceptance of an employment contract linked to this post constitutes agreement to deploy. The work is normally performed in a typical Office environment. Normal Working Conditions apply. The risk of injury is categorised as: No risk / risk might increase when deployed.

The successful candidate has the following qualifications

Professional Education
- Higher Secondary education and intermediate vocational training in computer science, engineering disciplines, statistics or similar numerate discipline, operations research or related discipline with 2 years' experience, or Secondary education and completed advanced vocational training in that discipline leading to a professional qualification or professional accreditation with 4 years related experience.
- Certification in Information Assurance or CIS security (Security+, CCNA Security or similar)
- Professional certification in Windows or Linux operating systems
- Good Command of English.

Professional Experience in
- Minimum two years practical experience in system and network administration of both Microsoft and UNIX LINUX environments.
- Proven knowledge of TCP/IP stacks protocols and ports.
- Work experience in computer security tools and vulnerability assessment methodologies.
- Minimum 2 years of experience providing Information Assurance support.
- Comprehensive knowledge of the principles of computer and communications security, networking, and the vulnerabilities of modern operating systems and applications.

Preferred qualifications are
- Experience providing on the job training.
- Experience providing Information Assurance support to operations and exercises.
- Professional certification in networking (CCNA, CCNP or similar).
- Experience working with LAN Technologies / LAN Switching / WAN Technologies / Switches & Routers.
- Experience working with the McAfee e-Policy Orchestrator management suite and endpoint security applications.
- Experience working with SIEM applications.
- COMPUSEC Practitioner course.
- ITIL v3 Foundation Certification.
Personal Attributes
The successful candidate:
✓ is able to work under pressure
✓ is a very good team-player
✓ has good communication skills

The successful selected candidate needs to complete a NATO medical examination and obtain a NATO security clearance before an employment offer will be released. The medical examination will take place with our medical consultant and is required to determine if the recommended candidate is fit to perform the duties of the position and is deployable to NATO’s regional areas of operation.

Newly recruited staff members will be offered a definite duration contract of 3 years, including a 6 months probationary period. Unless organisational reasons prevent and assuming satisfactory performance, after the 3 year contract has expired staff members will normally be offered an indefinite duration contract.

DUE DATE for receipt of applications: 4 March 2020 COB

Applicants are required to apply electronically through NTAP: https://nato.taleo.net/careersection/1/jobsearch.ftl?lang=en

Results of the initial screening for this post may be expected by in the second week of March 2020. Test and interviews are planned last week of March 2020 and will take place in Wesel, Germany. The interview scheme might include a HireVue and/or other (written) test.