NATO | OTAN

NORTH ATLANTIC TREATY ORGANIZATION
INTERNATIONAL STAFF

ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD
SECRÉTARIAT INTERNATIONAL

VACANCY NOTIFICATION/ NOTIFICATION DE LA VACANCE DU POSTE

Technician, Cybersecurity (210605)

Primary Location Belgium-Brussels
NATO Body NATO International Staff (NATO IS)
Schedule Full-time
Application Deadline 31-Aug-2021
Salary (Pay Basis) 3,498.71Euro (EUR) Monthly
Grade NATO Grade G8-G10
Clearance Level CTS
Description

1. SUMMARY

The BICES Group Executive (BGX), a NATO entity, is the executive body of the BICES Group (BG). The BG exists to enable the sharing and exchange of Intelligence and Information between and amongst the NATO nations and with NATO, and with other non-NATO nations and Organizations. The BGX, under the leadership of the Director BGX, is comprised of the following pillars: Intelligence Service Strategy (ISS) Division, Intelligence Service Design (ISD) Division, Intelligence Service Operation (ISO) Division, and the Intelligence, Surveillance and Reconnaissance (ISR) Cell and the Security Office.

The Network Cyber Defence (NCD) section, under the Security Office, primarily exists to assure the confidentiality, integrity, and availability of BGX provided data and information, through cybersecurity means. The section is responsible to perform the daily network-based, cybersecurity activities within the BGX, which include, but are not limited to, manual and automated CIS monitoring, incident response, mitigation and reporting, risk assessment and mitigation, hardware and software-based system hardening, security awareness.

Under the supervision of the Head, NCD and in close coordination with the Cybersecurity Officers and Engineers, the incumbent will provide 1st and 2nd level support for complex technical cybersecurity-based activities in the area of network defence monitoring and incident response. S/he will also contribute to the day-to-day monitoring, updating, and baselining of the cybersecurity capabilities currently implemented within the BGX/BICES networks. The incumbent will report the status of the security posture of BICES networks following the Incident Response chain of command and will play an active role in any/all monitoring, changes and modification on security services.

2. QUALIFICATIONS AND EXPERIENCE

ESSENTIAL

The incumbent must:

- have a good general education at least to higher secondary level in information technology or security, or similar;
- possess at least 3 years' previous experience in CIS security activities;

- have detailed knowledge of Windows- and Linux-based operating systems, of the Windows Server Update Service (WSUS) and of IP-based network and router;
- have knowledge of firewall and intrusion detection technology;
- have the ability to identify and describe computer and network anomalies within a CIS and to understand, assess and solve technical issues;
- have experience with security tools like firewalls, proxies, guard technology, NESSUS, Splunk, etc;
- have knowledge of SOC processes and procedures;
- have detailed knowledge on vulnerability assessment and penetration testing techniques;
- have detailed knowledge on log fusion and log analysis capabilities;
- possess an upper-intermediate level (IV) of English.

DESIRABLE

The following would be considered an advantage:

- an advanced level of English, both oral and written;
- knowledge of NATO security policy and supporting directives;
- experience working in a multinational environment;
- experience with the application of techniques/methods for source verification, data fusion, quality analysis, and threat actor profiling;
- knowledge of software development with experience in writing code/scripts;
- a beginner level (I) in French.

3. MAIN ACCOUNTABILITIES

Expertise Development

Provide essential broad scope and depth of cybersecurity knowledge necessary to function within the environment, contributing knowledge and experience to the continued success of the organizational and team objectives.

Information Management

Parse and report triaged artifacts to NCD chain of command, so as to provide actionable information in a timely manner that will be used by Incident Response teams for appropriate investigative action. Provide Cybersecurity Engineers with additional support in Security Test & Verification (ST&V) activities.

Planning and Execution

Support and maintain the continual monitoring activities of the BICES classified and unclassified networks. Perform triage on any anomalies and network artifacts (i.e., alerts, thresholds, alarms, etc.) that are produced via the Security Information and Event Management (SIEM) and the Central Log Management systems, prioritizing and categorizing said artifacts.

Project Management

Provide support to the design, documentation, testing and implementation of assigned projects, to include all stages of the implementation process.

Stakeholder Management

Promote and maintain professional relations with appropriate counterparts, both military and civilian, within nations, NATO and other international organisations as required. Maintain contacts with system software and hardware vendors and/or contractors for software and hardware new releases and/or updates.

Perform any other related duty as assigned.

4. INTERRELATIONSHIPS

The incumbent reports to the Head NCD (Security Operation), for all aspects of NCD (Security Operation) within the scope of the BICES Group (BG) and the wider BICES Community.
Direct reports: N/A
Indirect reports: N/A

5. COMPETENCIES

The incumbent must demonstrate:

- **Achievement:** Works to meet standards. Works to meet expected performance at standards set by others (management or customers).Executes duties in a timely, efficient and accountable fashion and meets objectives within target dates. May express frustration at waste or inefficiency.
- **Analytical Thinking:** Breaks down problems. Makes a list of items that need doing, with no particular order or set of priorities. Pulls together data, ideas, issues and observations into a clear and useful format.
- **Customer Service Orientation:** Takes personal responsibility for correcting problems. Takes ownership of the correction of customer-service problems. Corrects problems promptly, efficiently and without becoming defensive. Monitors client satisfaction.
- **Flexibility:** Acts with flexibility. Works effectively in a changing environment. Adapts to change by actively revising own behaviours, methods and priorities. Applies procedures flexibly, where context allows, in order to get a job done or to meet agreed objectives (e.g. alters normal procedures to fit a specific situation and to meet a client's needs).
- **Initiative**: Is decisive in a time-sensitive situation. Acts quickly and decisively in a crisis or other time-sensitive situation. Is unafraid to propose and/or take action when the norm would be to wait, study the situation and hope the problem will resolve itself.
- **Organizational Commitment:** Supports the Organization. Acts to support the Organization’s mission and goals. Makes choices and sets priorities to meet the Organization’s needs and to align self with its mission.
- **Self-Control:** Responds calmly. Remains patient, does not show frustration. Continues to act calmly under pressure or while experiencing strong emotions. Rises above the situation and diffuses other’s negative emotions.
- **Teamwork:** Cooperates. Participates willingly in the team, doing his/her share of the team’s work. Shares information and knowledge freely, offering support and cooperation.

6. CONTRACT

Contract clause applicable:
This is a limited duration project post. The incumbent will be offered a definite duration contract of one year, with the possibility of extension, subject to funding and project requirement. The first 3 months of the contract will be considered as a probationary period.

Serving staff will be offered a contract in accordance with the NATO Civilian Personnel Regulations.

NOTE: Irrespective of previous qualifications and experience, candidates for twin-graded posts will be appointed at the lower grade. Advancement to the higher grade is not automatic, and will not normally take place during the first three years of service in the post.

Under specific circumstances, serving staff members may be appointed directly to the higher grade, and a period of three years might be reduced by up to twenty four months for external candidates. These circumstances are described in the IS directive on twin-graded posts.

7. RECRUITMENT PROCESS

Please note that we can only accept applications from nationals of NATO member countries. Applications must be submitted using e-recruitment system, as applicable:

- For NATO civilian staff members only: please apply via the internal recruitment portal (link);
- For all other applications: www.nato.int/recruitment

Please note that at the time of the interviews, candidates will be asked to provide evidence of their education and professional experience as relevant for this vacancy.

Appointment will be subject to receipt of a security clearance (provided by the national Authorities of the selected candidate) and approval of the candidate's medical file by the NATO Medical Adviser.
More information about the recruitment process and conditions of employment, can be found at our website (http://www.nato.int/cps/en/natolive/recruit-hq-e.htm).

8. ADDITIONAL INFORMATION

NATO is committed to diversity and inclusion, and strives to provide equal access to employment, advancement and retention, independent of gender, age, nationality, ethnic origin, religion or belief, cultural background, sexual orientation, and disability. NATO welcomes applications of nationals from all member Nations, and strongly encourages women to apply.

Building Integrity is a key element of NATO's core tasks. As an employer, NATO values commitment to the principles of integrity, transparency and accountability in accordance with international norms and practices established for the defence and related security sector. Selected candidates are expected to be role models of integrity, and to promote good governance through ongoing efforts in their work.

Due to the broad interest in NATO and the large number of potential candidates, telephone or e-mail enquiries cannot be dealt with.

Applicants who are not successful in this competition may be offered an appointment to another post of a similar nature, albeit at the same or a lower grade, provided they meet the necessary requirements.

The nature of this position may require the staff member at times to be called upon to travel for work and/or to work outside normal office hours.

The organization offers several work-life policies including Teleworking and Flexible Working arrangements (Flexitime) subject to business requirements.

Please note that the International Staff at NATO Headquarters in Brussels, Belgium is a non-smoking environment.

For information about the NATO Single Salary Scale (Grading, Allowances, etc.) please visit our website. Detailed data is available under the Salary and Benefits tab.