NATO | North Atlantic Treaty Organization
International Staff

OTAN | Organisation du Traité de l'Atlantique Nord
Secrétariat International

VACANCY NOTIFICATION/ NOTIFICATION DE LA VACANCE DU POSTE

IA Operations Officer (180594)

Primary Location
Belgium-Brussels
NATO Body
NATO International Staff (NATO IS)
Schedule
Full-time
Application Deadline
20-Aug-2018
Salary (Pay Basis)
5,365.51Euro (EUR) Monthly
Grade A.2/A.3
Clearance Level CTS
Description

1. RESPONSIBILITIES OF THE POST:

- Responsible to the Head Information Assurance & Cyber Defence (IA&CD) for all duties allocated to him/her.
- Responsible to support BICES Exercise activities and to maintain a technical security oversight and compliance assessments of BICES installations of the BICES Group Executive (BGX), including the management of security incident handling activities.

2. DUTIES

- Support the technical cyber aspects of BICES Exercise including the BICES Exercise Environment (BEXEN).
- Manage and execute log information analysis of BGX operated services to identify potential cyber security related anomalies, and provide analytical reports.
- Support and provide cyber status briefings with potential impact and recommendations to BGX Management.
- Conduct vulnerability assessment activities, including reporting.
- Provide assessments and practical solutions for identified security incidents.
- Lead the BICES security incident management process.
- Lead the BICES Patch Management process.
- Maintain the BICES Cyber Defence related standard operating procedures.
- Support the analysis of current and new services/functionalities on BICES with respect to Cyber Defence related requirements.

- Liaise with Intelligence Service Strategy (ISS) exercise planner.
- Liaise with Intelligence Service Operation (ISO) technical experts (Technologists, Senior Technicians and Technicians) in support of security incident solving activities.
- Participate, when assigned by the BICES Programme Management Board (BPMB) (in the security related aspects of projects for Capability Development).
- Participate to ISO configuration and implementation activities in the areas of network equipment, firewalls, service guards and host based information assurance components.
- Support security inspection activities.
- Implement, maintain and improve Cyber Defence mechanisms.
- Support any urgent matters.
- To cooperate and coordinate Computer Information Systems (CIS) security aspects with national/organisational experts, including NATO Computer Incident Response Capability (NCIRC) Technical Centre and Exercise Planning Teams.
- To represent the BGX at meetings of national, NATO or other international bodies as required.
- To represent the Information Assurance Office in official meetings.
- To liaise with national, NATO or other international bodies and individuals as required.

3. QUALIFICATIONS AND EXPERIENCE

Essential

- Minimum 3 years proven experience in CIS security activities.
- A university degree in information technology or engineering with a core area in information technology, or similar.
  Familiar with:
- NATO and/or national intelligence systems.
- Communications and information systems project management techniques.
- Communications and information systems design.
- Ability to understand, assess and solve complex technical security issues.
- Proven ability to communicate effectively orally and in writing with good briefing skills.
- Sound capacity to deal and negotiate with Nations.
- Knowledge of information management techniques.
- Detailed knowledge of Local Area Network (LAN) and Wide Area Network (WAN) communications, with the ability to define, design and implement communications infrastructures.
- Detailed knowledge of router-based networks.
- Detailed knowledge firewall and guarding technologies.
- Detailed knowledge on vulnerability assessment techniques.
- Detailed knowledge on log fusion and log analysis capabilities.

Desirable

- Knowledge of NATO security policy and supporting directives.
- Post graduate experience in computer engineering or information management systems, or equivalent combination of appropriate qualifications and experience.
- Experience working in a multinational environment.

- A working knowledge of NATO organisations and procedures.
- Awareness of best practices/Information Technology Infrastructure Library (ITIL) methodology and its implementation.
- Experience in the Cyber Defence field.
- Knowledge of BICES environment.

4. LANGUAGE PROFICIENCY

Must be fluent orally and in writing in one of the official languages of the Organisation; a working knowledge of the other is desirable. (Note: most of the work, both oral and written, in this post, and in BGX as a whole, is conducted in English).

5. PERSONAL ATTRIBUTES

- Personal qualities of tact, judgement and adaptability.
- A sense of diplomacy and propriety in order to work harmoniously with colleagues, both military and civilian, and more particularly from nations and from NATO.

6. PROFESSIONAL CONTACTS

Establish and maintain professional relations with appropriate officials, both military and civilian, within nations, NATO and other international organisations as required and in particular to be able to carry out his main duty dealing with accreditation.

7. SUPERVISORY/GUIDANCE DUTIES

- To supervise IA Operations activities with assigned personnel.
- To supervise BGX CIS security aspects in relation to a communications and information system as directed.
- To give Computer Information Systems (CIS) security related guidance to BGX personnel involved in the operation and development of a communications and information systems.
- To coordinate and give CIS security related guidance as necessary to the appropriate personnel of the BICES Community.
- Ability to manage a team.

8. WORKING ENVIRONMENT

- Normal office environment.
- Working in fielded environments might be necessary for shorter periods.

9. TRAVEL REQUIREMENTS

Some travel is required.

10. CONTRACT:

The successful applicant will be offered a 3-year definite duration contract, which may be renewed for a further period.

If the successful applicant is seconded from the national administration of one of NATO's member States, a 3-year definite duration contract will be offered, which may be renewed for a further period subject also to the agreement of the national authority concerned.

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.
There are certain specific circumstances in which a serving staff member may be appointed directly to the higher grade. These are described in the IS directive on twin-graded posts. Advancement to the higher grade is not automatic and at least a minimum period of 3 years' service (2 years for an A.1/A.2 post) is required before promotion to the higher grade can be considered.

11. RECRUITMENT PROCESS:

Applications must be submitted using e-recruitment system, as applicable:

- For NATO civilian staff members only: please apply via the internal recruitment portal (for more information, please contact your local Civilian HR Manager);

Selective assessments: beginning of September
Final assessments: beginning October

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)

12. ADDITIONAL INFORMATION:

NATO as employer values diverse backgrounds and perspectives and is committed to recruiting and retaining a diverse and talented workforce. NATO welcomes applications of nationals from all Member States 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.