SUPREME HEADQUARTERS ALLIED POWERS EUROPE

TALEO Job Number: 220210

Vacancy Number: A08/0322

Post Number: OSC CODX 0040

Job Title: Engineer (Vulnerability Analysis)

NATO Grade: 15

Basic Monthly Salary (12 x per year): 5.735,66 €, tax free

Closing Date: Sunday 3 July 2022

NATO Communications and Information Systems Group (NCISG) is looking for an experienced and qualified Engineer (Vulnerability Analysis) to join a professional team providing technical coordination for Deployable Communication Information Systems in Cyber Defence(CD). The individual will be responsible for the vulnerability management and engineering preventive Cyber Defence capabilities within the Allied Command Operations (ACO). If you enjoy working in a fast pace international environment involving frequent travel and deployments, this post is for you.

GENERAL BACKGROUND:

SHAPE, the Supreme Headquarters Allied Powers Europe, is the Headquarters of Allied Command Operations (ACO), one of the two major military commands of the North Atlantic Treaty Organisation (NATO). ACO safeguards an area extending from the northern tip of Norway to the eastern border of Turkey. This equates to nearly two million square kilometres of land, more than three million square kilometres of sea, and a population of about 320 million people.

POST DESCRIPTION:

Location: Casteau/Mons, 60 Km south of Brussels (Belgium)
Division: Office of Chief of Staff

POST CONTEXT/POST SUMMARY

The J2/6 Division is the technical coordination authority for Deployable Communication Information Systems and is responsible for the operational integration, coordination, direction and provision of required technical services for the NATO Communications Information Systems Group and NATO Signal Battalions.
The Information Assurance and Cyber Defense Branch is responsible for all aspects of NATO Communications Information Systems Group organizational security and Deployable Communications Information Systems Information Assurance, to include the planning, coordination and operational integration of Defensive Cyberspace Operations and Cyberspace Intelligence.

The Defensive Cyberspace Operations Section is responsible for planning, preparing, and executing all lifecycle management activities of Deployable Communication Information Systems Cyberspace Defence, and providing guidance and coordinating Defensive Cyberspace Operations operational integration to the NATO Signal Battalions. The incumbent serves as the NCISG Cyber Defence (CD) Subject Matter Expert responsible for vulnerability management and engineering preventive CD capabilities for the Deployable CIS (DCIS).

PRINCIPAL DUTIES

The incumbent's duties are:

1. Responsible to the NCISG J2/6 IACD DCO Section Head for DCIS Vulnerability Management.
2. NCISG CD Subject Matter Expert responsible for vulnerability management, cyber hygiene and engineering preventive CD capabilities for DCIS.
3. Interfaces with NCIA, NCISG HQ counterparts and NCISG subordinate units to ensure resilience of the DCIS CD capabilities in accordance to the Minimum Military and FMN requirements.
4. Assists in translating the ACO Operational Requirements into DCIS CD related directives and guidance documents and develop internal NCISG procedures.
5. Supports the provision of CD services to operations and exercises. Provides Level 2 Cyber Defense support to Deployed CIS.
6. Provides Engineering support to DCIS CD Situational Awareness and Consequence Management for NATO Operations and exercises.
7. Engineers and recommends CD architectural & procedural modifications to assist in mitigating risks & vulnerabilities identified during vulnerability assessments, Penetration Testing, and in support of Incident and Vulnerability Management findings.
8. Manages the NCISG responses to identified vulnerabilities in coordination with other partner organizations to prevent malicious activities from affecting federated networks and responds to vulnerabilities when required.
9. Develops and maintains processes and procedures in areas of functional expertise and coordinates within NCISG HQ and with subordinate units to ensure compliance.
10. Writes detailed problem reports, assessment plan documents and mitigation recommendations as needed.

SPECIAL REQUIREMENTS AND ADDITIONAL DUTIES

The employee may be required to perform a similar range of duties elsewhere within the organization at the same grade without there being any change to the contract
Mandatory Deployment Post. The incumbent may be required to undertake deployments in support of military operations and exercises, and/or TDY assignments, both within and outside NATO boundaries. Such operational deployment may exceed 30 days duration up to 183 days in any period of 547 days and may be on short notice. For NATO International Civilian Staff, acceptance of an employment contract linked to this post constitutes agreement to deploy in excess of 30 days if required.

- May be required to participate in NATO policy and publication maintenance and capability development in functional areas of expertise.
- May be required to augment the NCISG DCC or DSG DNOC providing cyberspace vulnerability engineering support to NATO operations and exercises.

The work is normally performed in a NATO office environment.
Normal Working Conditions apply.
The risk of injury is categorized as: No Risk.

ESSENTIAL QUALIFICATIONS

A. Professional/Experience

1. Minimum two years of engineering experience in vulnerability assessment, vulnerability management and remediation.
2. Minimum two years of experience in the design, implementation and deployment of enterprise vulnerability assessment and management solutions.
3. Experience in identifying vulnerabilities in web-based applications and databases.
4. Experience in the development of CIS Security Standard Operating Procedures and technical guidance.
5. Proficient in the analysis of Cyberspace Threats and the implementation of mitigation techniques.
6. Experience leading small teams and mentoring junior analysts/technicians.
7. General certification in Information Assurance or CIS security (Security+, GSEC, CEH, CISSP or equivalent).

B. Education/Training

University Degree in computer science, engineering disciplines, statistics or similar numerate discipline, operations research or related discipline and 2 years function related experience, or Higher Secondary education and completed advanced vocational training in one of the disciplines mentioned above leading to a professional qualification or professional accreditation with 4 years post related experience.

C. Language

English - SLP 3322 (Listening, Speaking, Reading and Writing)
NOTE: The work both oral and written in this post and in this Headquarters as a whole is conducted mainly in English.

DESIRABLE QUALIFICATIONS

A. Professional Experience

1. Knowledge with NATO Cyber Defense and CIS security policies.
2. Experience with a recognised Enterprise Risk Management methodology.
3. Experience in secure network architecture and design.
4. Four years of experience administering and securing Microsoft Windows-based client and server systems.
5. Two years of experience administering and securing Unix and Linux-based systems.
6. Extensive experience in the use of online Vulnerability Assessment tools, preferably Tenable.SC and Nessus.
7. Work experience in Cyberspace Operations Centres.
8. Experience with industry-standard SIEM solutions, preferably Splunk enterprise Security.
9. Experience providing CIS support to military operations and exercises.

B. Education/Training

1. University Degree in Information Technology or Cyber Security at a nationally recognized university and 4 years of function-related experience.
2. Certification in prevention techniques (GCCC or other equivalent).

ATTRIBUTES/COMPETENCIES

A. Personal Attributes

The incumbent will need to display a high degree of initiative, professionalism and engineering expertise in performance of his/her duties. The rapidly changing NATO environment creates a requirement to solve numerous complex problems and challenges, which shall require the incumbent to draw upon a comprehensive ability to

quickly reason, analyze, act with persuasion and diplomacy. Requires a high degree of tact and perseverance to ensure that technically sound decisions are made in a timely manner in reaction to current events. The incumbent must be able to use own initiative with minimal supervision and be able to lead a small functional team, both physical and virtual, in order to implement, manage, and maintain strategies and procedures to timely reduce and prevent network vulnerabilities.
- The incumbent will be required to maintain an adequate degree of physical fitness to comply with NATO deployability requirements.
- The incumbent may be required to travel away from his/her duty location for extended periods in support of NATO operations and exercises

B. Managerial Responsibilities

The incumbent serves as the primary point of contact and subject matter expert on the issues related to Cyber Defense vulnerabilities; that is, the immediate and long-term actions related to identifying and correcting network areas vulnerable to cyber-attack on the deployed network. As such, the incumbent develops and implements cyber defense strategies and procedures and is responsible for the coordination, immediate implementation and maintenance of these strategies and procedures by the NATO Signal Battalion cyber defence technicians.

C. Professional Contacts

Professional Contacts: Regular professional contacts with others inside and/or outside immediate organization on functional matters. Solicits/provides information and assessments/advice in functional area of expertise within the organization. Present and support coordinated NCISG viewpoints and decisions regarding functional area of expertise to others outside the organization.
Deputy SSG DNOC CD Cell Head.

D. Contribution To Objectives

Work involves the provision of information, analysis, and engineering technical solutions for the defence of the DCIS network provided by the organization, compelling others within the organization to action within the SSG/DNOC. The incumbent is the lead in assessing the potential vulnerabilities to a cyber-attack of a deployed network and will commit the cyber defence functional area of NCISG to numerous courses of action in defense of the network, affecting NCISG's mission accomplishment in DCIS provision.
This post reports to
• OCG CODX 0010 - Section Head (Defensive Cyberspace Operations) - A3/G17
• Supervisory Responsibilities: None.

REMARKS:

Duration of contract: Serving staff members will be offered a contract according to the NATO Civilian Personnel Regulations (NCPR). Newly recruited staff will be offered a definite duration contract of three years normally followed by an indefinite duration contract.

HOW TO APPLY FOR A NATO CIVILIAN POST AT SHAPE:

Applications are to be submitted using NATO Talent Acquisition Platform (NTAP) (https://nato.taleo.net/careersection/2/jobsearch.ftl?lang-en). Applications submitted by other means (e.g. mail, e-mail, fax, etc) are not accepted.

A copy of the qualification/certificate covering the highest level of education required by the job description must be provided as an attachment.

Essential information must be included in the application form. Expressions such as “please see attached CV, please see annex / enclosed document” or invitations to follow links to personal webpages are not acceptable and will be disregarded. All answers should be in English.

Shortlisted candidates will be requested to provide original documentary evidence and a set of copies supporting statements in their applications. Appointment is subject to obtaining a CTS-A security clearance and a medical certificate.

Remarks:
A) Only nationals from the 30 NATO member states can apply for vacancies at SHAPE.
B) Applications are automatically acknowledged within one working day after submission. In the absence of an acknowledgement please make sure the submission process is completed, or, re-submit the application.
C) Qualified redundant staff of the same grade interested in this post should inform this office, via their HR/Personnel Office by not later than vacancy’s closing date.
D) Candidates’ individual telephone, e-mail or telefax enquiries cannot be dealt with. All candidates will receive an answer indicating the outcome of their application.