SUPREME HEADQUARTERS ALLIED POWERS EUROPE

TALEO Job Number: 241264

Vacancy Number: G137/24

Post Number: OCG COAX 1010

Job Title: Engineer (CIS Security)

NATO Grade: G15

Basic Monthly Salary (12 x per year): 6,118.54€, tax free

Closing Date: Monday 16 September 2024

POST CONTEXT/POST SUMMARY

Supreme Headquarters Allied Powers Europe (SHAPE) provides an integrated Strategic Effects framework, employing a multi-domain and multi-region focus to create a 360-degree approach, with the flexibility to enable, upon direction, a seamless transition from Baseline Activities and Current Operations (BACO) up to the Maximum Level of Effort (MLE). SHAPE supports the Supreme Allied Commander Europe (SACEUR) in fulfilling his terms of reference, as directed by the North Atlantic Council.

The NATO CIS Group conducts CIS operational planning and provides deployed/deployable CIS services and support in support of NATO military operations and exercises. The NATO CIS Group is located at SHAPE, the Headquarters of Allied Command Operations (ACO), one of the two major military commands of the North Atlantic Treaty Organisation (NATO).

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 Defence 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 Information Assurance and Security Services Section is responsible for Deployable Communication Information Systems Information Assurance and security engineering, and the enforcement of the NATO security policy throughout NATO Communications Information Systems Group.

The incumbent is responsible to support the operational integration of the DCIS Cyber Defence capabilities that are provided as part of the NATO 2030 Digital Backbone in order to protect NATO mission networks. The incumbent will work in close coordination with NCISG administrators and operational users of these capabilities to enable the achievement of the NATO 2030 Digital Backbone targets for readiness and resilience.

PRINCIPAL DUTIES

The incumbent's duties are:

1. CIS Security Officer for the NATO 2030-provided DCIS Cyber Defense capabilities.

2. Leads the operational integration of the NATO 2030 DCIS CD Capabilities from a security compliance and accreditation perspective.

3. Ensures that the NATO 2030 DCIS Cyber Defense capabilities are in compliance with NATO security policy.

4. Performs regular design and process reviews in coordination with his / her counterparts.

5. Performs all tasks related with the CIS security accreditation and certification of the NATO 2030 DCIS Cyber Defence capabilities.

6. Develops CIS security operations procedures (SecOPs) and ensures the linked projects are aligned with NATO security best practices.

7. Identify CIS security problems and gaps, as well as projects systems weaknesses.

8. Performs periodic CIS security tests and validates that the CIS security controls meet NATO 2030 performance targets.

9. Ensures adherence to the NATO security policies and standards.

10. Maintains a security configuration database and periodically reports to the accreditation authority.

11. Maintains professional contacts with relevant stakeholders inside and outside NCISG.

SPECIAL REQUIREMENTS AND ADDITIONAL DUTIES

1) The incumbent may be required to undertake deployments in support of military operations and exercises, and/or TDY assignments, both within and without NATO boundaries up to 180 days. 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.

ESSENTIAL QUALIFICATIONS

A. Professional/Experience

1. Minimum 2 years of work experience as a CIS security officer.
2. Minimum 2 years of work experience supporting CIS security accreditation activities.
3. Theoretical knowledge and practical experience in Information Security concepts and technology.
4. Demonstrable knowledge of secure network architecture design.
5. Experience authoring documentation and in configuration management.
6. Experience administering or auditing Microsoft Windows systems.
7. Experience administering or auditing Linux-based systems.
8. Experience administering or auditing network devices.
9. General certification in Cyber security or auditing (Security+, SSCP, GSEC, or equivalent).

B. Education/Training

1. University Degree in business administration, engineering, economics, public administration, operations research, business process engineering or related discipline and 2 years post related experience, or Higher Secondary education and completed advanced vocational training in that discipline leading to a professional qualification or professional accreditation with 4 years post related.

C. Language

English - SLP 3333 - (Listening, Speaking, Reading and Writing)

DESIRABLE QUALIFICATIONS

A. Professional Experience

1. Five years of experience in CIS security roles.
2. Work experience in a security certification / accreditation role in a military organization, international organization or corporation.
3. Work experience as a Systems Administrator managing a large and diverse IT infrastructure.
4. Experience auditing computer systems and networks.
5. Experience in risk assessment using industry-standard tools.

6. Work experience with Redhat Linux is highly desirable.

7. Work experience with Cisco firewalls is highly desirable.

B. Education/Training

1. Cisco CCNA Security Certification.

2. ISACA CISA or CRISK certification.

3. CISSP / CISM or equivalent certification.

4. NATO C4ISR Orientation for Officers (CCC-SM-22206) provided by NATO Communications and Information Academy (NCI Academy).

5. NATO Orientation Course (ETE-MW-3834) provided by NATO - School Oberammergau (NSO).

ATTRIBUTES/COMPETENCIES

1. Personal Attributes: The incumbent is to be a talented CIS security engineer ready to be challenged on a daily basis to support the operational integration of innovative Cyber security solutions that are used to protect NATO's mission networks. Must be adaptable to continuously changing requirements. Must be able to think out of the box and to challenge the way things are done with excellent teamwork abilities. Must be result-oriented, efficient and assertive but at the same time tactful and respectful to others.

2. Professional Contacts: Regular professional contacts with others inside and/or outside immediate organisation on functional matters. Solicits/gives information and provides advice/guidance.

3. Contribution To Objectives: Work involves the provision of information or analysis of part of a task assisting others to take action within the organization.

REMARKS:

Duration of contract: The successful candidate will fill this post as a Project Related NATO International Civilian (PLN) with a three-year definite duration contract within the NATO 2030 Agenda. On expiry of this term the PLN will be deleted or absorbed into the ceiling pending approval or will exceptionally be considered for extension.

The salary will be the basic entry-level monthly salary defined by the NATO Grade of the post, which may be augmented by allowances based on the selected staff member's eligibility, and which is subject to the withholding of approximately 20% for pension and medical insurance contributions.

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.

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.

Applicants who prove to be competent for the post but who are not successful in this competition may be offered an appointment in another post of a similar nature, which might become vacant in the near future, albeit at the same or lower grade, provided they meet the necessary requirements.

We believe that all people are capable of great things. Because of this, we encourage you to apply even if you do not meet all of the criteria listed within this job description.

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.

More information to be found on these links:

6 Tips for Applying to NATO

Application Process

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 NS security clearance and a medical certificate.

Remarks:

A) Only nationals from the 32 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) NATO will not accept any phase of the recruitment and selection prepared, in whole or in part, by means of generative artificial-intelligence (AI) tools, including and without limitation to Chatbots, such as Chat Generative Pre-trained Transformer (Chat GPT), or other language generating tools. NATO reserves the right to screen applications to identify the use of such tools. All applications prepared, in whole or in part, by means of such generative or creative AI applications may be rejected without further consideration at NATO's sole discretion, and NATO reserves the right to take further steps in such cases as appropriate.