SUPREME HEADQUARTERS ALLIED POWERS EUROPE

Vacancy Number: 240243

Job Title: Senior Risk Manager

Post Location: Casteau/Mons, 60 Km south of Brussels (Belgium)

Grade: 15

Basic Monthly Salary: EUR 6,118.54

Closing Date: Thursday 29 February 2024

Are you looking for an opportunity to work at the heart of NATO cyberspace operations? Then this opportunity might be for you!

1. POST CONTEXT

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 SACEUR in fulfilling his terms of reference, as directed by the North Atlantic Council.

The Cyberspace Directorate directs monitors and coordinates all Cyberspace Operations (CO), Electronic Warfare (EW), Electro Magnetic Spectrum (EMS) activity and Communications and Information Systems (CIS) functional area activities and staff functions across ACO.

The Cyberspace Operations Centre (CyOC) is NATO's only Theatre Component for cyberspace, providing persistent, centralised and comprehensive cyberspace situational awareness, Command and Control (C2) and execution. The CyOC is within the SHAPE establishment but with different roles and responsibilities.

The Cyberspace Operations Branch will be the means by which the Cyberspace Operations Centre (CyOC) will coordinate the full spectrum of NATO military activity within cyberspace.

The Cyberspace Defence and Effects Section defines, coordinates and manages ACO Cyberspace Defence across SACEUR's Area of Responsibility (AOR).

The incumbent is responsible for conducting the risk management at CyOC level involving all stakeholders susceptible to identify, assess and respond to risks in cyberspace.

2. PRINCIPAL DUTIES

The incumbent's duties are:

1) Conduct the risk management at CyOC level involving all stakeholders susceptible to identify, assess and respond to risks in cyberspace;
2) Translate and synthesize technical, intelligence, threat and blue force picture information, in context, and craft mitigation plans to ensure appropriate responses;
3) Support the development of response plans to the identified risks in order to ensure continuity of Alliance Operations and Mission (AOM) in a degraded and contested cyber environment;
4) Ensure that planned resilience and effective mitigation actions against consequence of cyber incident/attacks are implemented, executed, monitored and controlled;
5) Provide guidance on how to protect NATO CIS infrastructure and incorporating this in specific Direction and Guidance;
6) Ensure that corrective action is taken where risks response do not match expectations in order to improve the ability of commanders to operate in cyber degraded environments;
7) Support theatre-wide, operational risk management concerning cyberspace incidents that affect mission assurance (damage assessment - performance assessment - risk assessment - mitigation measures - consequence management);

3. SPECIAL REQUIREMENTS AND ADDITIONAL DUTIES

The employee may be required to perform a similar range of duties elsewhere within the organisation at the same grade without there being any change to the contract

1) Will be required to undertake operational assignment/secondment within SHAPE Multi Domain Operations Centre (may require shift work for the duration of the assignment);
2) Will be required to formally represent branch head or director at meetings;

3) Will be required to make presentations of the SHAPE position on cyberspace-related subjects/issues on behalf of branch chief or director;

4. ESSENTIAL QUALIFICATIONS

1. Professional/Experience

1) Minimum of 2 years of applicable experience in cyber and/or risk management, or a related field.
2) Proven ability to communicate effectively with stakeholders at all levels the identified risks and support the mitigation of risks.
3) Strong teamwork and collaborative skills. Ability to cooperate in a multi-national environment and to provide and accept feedback.

2. 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 that discipline leading to a professional qualification or professional accreditation with 4 years post related experience.

3. Language

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

5. DESIRABLE QUALIFICATIONS

1. Professional/Experience

1) Familiarity with ISO 2700-series or other security risk management framework.
2) Experience in concept development and planning of Consultation, Command and Control Systems.
3) Strong understanding of cybersecurity and technology risks, as well as relevant laws, regulations, and industry standards / frameworks (e.g. NIST CSF, SOC 2, ISO 27001, etc.);
4) Certifications/qualifications in cybersecurity, information systems, cloud, IT project management or data privacy.
5) Recent knowledge and experience of cyber and cyber defense capabilities in relation to support of the operations of a large international, governmental or military organization.

2. Education/Training

1) Hold at least one recognized professional qualification such as CISA, CISSP, CRISC;
2) Certified Information Systems Security Professional (CISSP)
3) Certified in Risk and Information Systems Control (CRISC)
4) Risk management courses (i.e. MoR and others)

6. ATTRIBUTES/COMPETENCIES

1) Personal Attributes: Able to work in a multinational environment.

   The incumbent will need to display a high degree of professionalism, technical expertise, organisational, coordination and communication skills in the performance of his/her duties. The rapidly changing NATO / CYBERSPACE environment and increasingly constrained resource situation creates a requirement to solve numerous complex problems and challenges, which shall require the incumbent to draw upon a comprehensive ability to reason, analyse, act with persuasion and diplomacy. The post requires a self-starter, analytical skills, ability to translate data and test results into evaluative conclusions, and conceptual thinker. Team worker. Must impact/ influence activities within the various stakeholders' organization.

2) Professional Contacts: The incumbent needs to develop very good working relationship with other entities such as the J6, NCISG, NCIA, CTAB, OCIO, NATO C3S, the NATO Office of Security, the NATO Office of Resources, and other various Host Nations, as well as Cyberspace staff within the subordinate Commands.
3) Contribution to Objectives: Ensure that the operational impact of risks and issues are rigorously and continuously assessed in order to provide information and knowledge necessary for the strategic assessment and advice on military response options related to cyber incidents/attacks whilst conducting AOM and to increase resilience against potential cyber incidents.

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.
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.

ADDITIONAL INFORMATION

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

NTAP allows adding attachments. 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. Particular attention should be given to Education and Experience section of the application form. The application should be in English.

Shortlisted candidates will be requested to provide original documentary evidence and a set of copies supporting statements in their applications.

After submitting your application, you will receive an acknowledgement of receipt of your application.

Remarks:
A) Only nationals from the 31 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) Candidates' individual telephone, e-mail or telefax enquiries cannot be dealt with. All candidates will receive an answer indicating the outcome of their application.