NATO DIANA
Defence | Innovation | Adoption

Vacancy Notice

Cybersecurity Lead-261285

Primary Location: London, United Kingdom
NATO Body: Defence Innovation Accelerator for the North Atlantic (DIANA)
Schedule: Full-time
Application Deadline: 24-Aug-2026, 10:59:00 PM (BST, London, UK)
Salary (Pay Basis): 7,646.99 Pound Sterling (GBP) Monthly
Grade: NATO Grade G17

The post is budgeted from 1 January 2027, and the successful candidate is expected to start employment as soon as possible thereafter.

1. OVERVIEW OF DIANA

NATO DIANA is the Defence Innovation Accelerator for the North Atlantic, a NATO body dedicated to finding and accelerating innovation to provide decisive defence and security effects for the Alliance, while fostering deep-tech innovation. NATO DIANA is comprised of a Board of Directors, representing all 32 nations, and an operational team referred to as the DIANA Executive ("DX"). Operating from three offices in Europe and North America, the DX leverages a network of military end users, world-leading accelerator sites, test centres, professional mentors and experts, and Allied expertise to accelerate the most innovative technologies from across the NATO Alliance. DIANA is a dynamic, agile workplace, which strives for innovative thinking, diversity, and performance excellence across all teams. To achieve our mission, DIANA is committed to providing our people with an environment that is positive, inclusive and collaborative.

2. OVERVIEW OF THE ROLE

The Safety, Security & Resilience (SSR) Team is responsible for safeguarding DIANA's people, information, facilities, and digital assets. The team develops and maintains proportionate frameworks, policies, controls, and assurance arrangements across cyber security, information security, physical security, safety, and security risk management to enable secure, safe, and resilient operations across DIANA. The Cybersecurity Lead is responsible for delivering DIANA's cyber security activities, ensuring the secure and resilient operation of its cloud, digital, and business technology services, along with cyber security architectural design. The role combines hands-on technical expertise with responsibility for cyber governance, risk

management, compliance, resilience, and assurance, embedding security by design across the organisation.

***Reserve candidates may be considered for similar posts in Estonia or Canada, if appropriate. ***

Reporting to DIANA's **Head of Safety, Security & Resilience.**

Duties of this role include:

- Lead the development, implementation and continual improvement of DIANA's cyber security, security architecture, governance framework, risk-management arrangements and assurance programme, building in security by design principles.
- Establish and manage cyber security policies, standards, control frameworks, risk registers, security metrics, and assurance documentation.
- Lead and oversee security risk assessments for DIANA Digital assets.
- Provide second-line challenge, oversight and assurance across technology projects, suppliers, cloud platforms, SaaS applications, AI solutions and operational processes, ensuring that risks are identified, assessed, treated and escalated appropriately.
- Lead cyber security incident response, assurance, and risk management activities, including for suppliers, service providers, and third-party technology partners.
- Lead internal and external audit, assurance, accreditation, and certification activities against relevant standards and assurance frameworks, including ISO/IEC 27001, NIST Cybersecurity Framework, NIST SP 800-53, Cyber Essentials Plus, CIS Benchmarks and applicable NATO security-accreditation expectations.
- Provide guidance, mentoring, or managerial leadership, as required, to enable collaboration, capability development, and successful delivery.
- Perform any other related duties as may be required.

3. ROLE REQUIREMENTS, QUALIFICATIONS AND EXPERIENCE

ESSENTIAL

The incumbent must have:

- A minimum requirement of a Bachelor's degree at a nationally recognised/certified University in Cyber Security, Information Security, Computer Science, Information Technology, Engineering, Digital Forensics, Networks, or a closely related technical discipline and 3 years post-related experience OR exceptionally, the lack of a university degree may be compensated by at least 10 years extensive and progressive expertise in duties related to the function of the post.
- A minimum of 3 years professional experience in cyber security, cloud security, security architecture, information assurance, or related technology-security roles.
- A recognized cyber security qualification (e.g. CISSP, CCSP, CCSK, or equivalent).
- Enterprise or security architecture qualifications (e.g. TOGAF or equivalent).
- Proven experience working in government, defence, law-enforcement, national security, critical infrastructure, NATO, or equivalent high-assurance sectors handling sensitive, regulated or classified information.
- Proven experience leading cyber security governance, risk management, assurance, security accreditation, audit, and control validation activities, including the application of recognised security standards, frameworks and principles.
- Proven experience in taking an organisation through ISO 27001 certification and other benchmarks such as Cyber Security Plus.
- Proven experience designing, implementing, securing, and assuring enterprise cloud and digital technology environments, particularly Microsoft Azure and Microsoft 365, including identity and access management, endpoint security, network security, monitoring and vulnerability management.
- Demonstrable experience assessing and managing cyber security risks across cloud services, SaaS platforms, suppliers, infrastructure, enterprise technologies, and business change initiatives.
- Experience providing disciplinary, project, or functional leadership, including setting priorities, managing resources, and delivering results through others.

- Possess the following minimum levels of NATO's official languages (English/French): V ("Advanced") in one; and I ("Beginner") in the other.

NOTE: Most of DIANA's internal work is conducted in the English language.

DESIRABLE

The following would be considered an advantage:

- A relevant postgraduate qualification, such as an MSc in Cyber Security, Information Security, Computer Science, Engineering, Digital Forensics, Artificial Intelligence, Cloud Computing, Risk Management, or a closely related discipline.
- Experience implementing advanced security technologies and capabilities, such as cloud security tooling, security monitoring and detection platforms, security automation, DevSecOps, AI governance, or enterprise security architecture.
- Knowledge of NATO institutional framework, policies and procedures.

COMPETENCIES

- The incumbent must demonstrate:
- Organizational and Environmental Awareness: *Understands the wider mission and considers the impact of their actions on others.*
- Initiative & Responsibility: *Takes ownership and accountability*.
- Adaptability & Flexibility: *Embraces change, adjusts priorities as needed, and continues to deliver results in evolving environments.*
- Impact & Influence: *Builds trust and buy in through confident and persuasive communication.*
- Stakeholder Management: *Builds strategic relationships and drives collaborative outcomes.*
- Leading & Developing Other: *Leads and develops others through coaching, empowerment, and feedback.*
- Self-awareness and a Learning Mindset: *Seeks opportunities to learn, reflects on experience, and applies learning to improve outcomes.*

4. WHAT WE OFFER

- Genuinely meaningful work as part of the newest unit within the most successful alliance in history.
- Tax-free salary.
- Household and children's allowances and privileges for expatriate staff including expatriation and educational allowances (where applicable) and additional home leave.
- Excellent private health insurance scheme.
- NATO pension scheme.
- Generous annual leave of 30 days plus official holidays.
- Flexible working conditions and a smoke-free office in London.
- Opportunities for learning and development.

5. CONTRACT

In accordance with the NATO Civilian Personnel Regulations, the successful candidate will receive a definite duration contract of three years, which may be followed by an extension. 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 of up to 3 years subject to the agreement of the national authority concerned. The maximum period of service in the post as a seconded staff member is six years.

6. USEFUL INFORMATION REGARDING APPLICATION AND RECRUITMENT PROCESS

Please note that we can only accept applications from nationals of NATO member countries. Applications must be submitted using the e-recruitment system, and any documents sent through other formats will not be reviewed (including email, social network, etc). Before you apply to any position, we encourage you to click here and review how to apply. Due to the broad interest in NATO DIANA and the large number of potential candidates, telephone or email enquiries cannot be dealt with. After review of your online application, successful candidates will be invited to a pre-recorded video interview. Shortlisted candidates from that will then be invited to the final assessments, which include: a language proficiency test, a job-related written test, and a panel interview. 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.

NOTE: DIANA 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, Copilot, Claude, etc.), or other language generating tools. DIANA 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 will be rejected without further consideration at DIANA's sole discretion, and DIANA reserves the right to take further steps in such cases as appropriate.

7. 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 is committed to fostering an inclusive and accessible working environment, where all candidates living with disabilities can fully participate in the recruitment and selection process. If you require reasonable accommodation, please inform us during your selection process along with documented medical evidence to support your request.
All NATO DIANA personnel are expected to conduct themselves in accordance with the current NATO Code of Conduct as agreed by the North Atlantic Council (NAC), and thus display the core values of integrity, impartiality, loyalty, accountability, and professionalism. The incumbent is required to be a resident in the host nation for the duration of their contract. DIANA has a flexible teleworking policy to permit working in office, at home, and across NATO Allied Nations subject to managerial approval.

For more information on DIANA, please visit our website.