

26735 - Network Security Tool Manager

Location: Mons, Belgium.

Period: 400 (start on 01 Dec. 2026)

Deadline: 06 Nov. 2026

Duties/Roles:

Security Tool Operations & Lifecycle Management:

- Deliver and maintain the network visibility and security monitoring capabilities required to support CSOC operations;
- Act as a subject matter expert for the operation, configuration, and lifecycle management of security monitoring and packet capture technologies;
- Manage the lifecycle of security monitoring platforms, including deployment, configuration, maintenance, upgrades, obsolescence management, and decommissioning;
- Configure, maintain, and optimize monitoring, traffic aggregation, and packet capture technologies to support reliable data collection and analysis;
- Monitor platform health, availability, data quality, retention, storage utilization, and operational performance;
- Identify and address visibility gaps that may impact threat detection or security operations;
- Maintain accurate documentation, architecture diagrams, inventories, operational procedures, and support information;
- Troubleshoot Linux, network, connectivity, performance, and data collection issues across the security monitoring environment.

Continuous Improvement

- Support the design and implementation of security monitoring solutions that align with CSOC requirements;
- Support integration with wider security operations, analytics, and incident management capabilities;
- Work with security analysts, detection engineering, and other stakeholders to improve monitoring coverage and support evolving detection requirements;
- Conduct capacity planning and scalability assessments to support future growth;
- Identify operational risks, improvement opportunities, and enhancements to increase reliability, visibility, and efficiency;
- Support compliance, audit, and assurance activities related to cyber defense technologies.

Stakeholder Engagement & Project Support:

- Provide subject matter expertise and technical guidance on security monitoring, network visibility, packet capture, and data collection requirements;
- Support projects and initiatives by ensuring monitoring and visibility requirements are considered during design, implementation, and service transition;
- Support cabling, deployment planning, and site survey activities related to security monitoring and network visibility infrastructure;
- Coordinate maintenance activities, vendor support engagements, and communications relating to platform status, risks, and improvement opportunities;
- If requested, participate in cyber defence related exercises supported by NCIA;
- Support the Defend Branch service delivery in the context of NCIA Enterprise Service Delivery Model and NCIA Customer Funded regime;
- Deputize for higher grade staff, if required;
- Performs other duties as may be required.

Skills, Knowledge, Experience Required:

Mandatory:

- The candidate must have a currently active NATO SECRET security clearance;
- A minimum requirement of a Bachelor's degree at a nationally recognised/certified University in a related discipline and 2 years post-related experience. Or exceptionally, the lack of a university degree may be compensated by the demonstration of a candidate's particular abilities or experience that is/are of interest to NCI Agency, that is, at least 6 years extensive and progressive expertise in duties related to the function of the post;
- Expert knowledge of network security monitoring, cyber defense operations, and enterprise security monitoring environments;
- Extensive hands-on experience supporting large-scale, distributed security monitoring deployments across multiple networks, sites, segments, or data centres;
- Hands-on enterprise experience with security monitoring and packet capture platforms such as Cisco Firepower, Corelight, and NetWitness;
- Proven experience in platform health monitoring, performance monitoring, capacity management, troubleshooting, and operational governance;
- Strong hands-on experience with network visibility, traffic aggregation, packet brokers, packet capture, and related monitoring technologies;

- Advanced understanding of enterprise networking concepts, protocols, architectures, and data flows;
- Linux and network troubleshooting experience, including connectivity, packet flow, interface, performance, and system-level diagnostics;
- Practical experience supporting cabling, site surveys, and physical deployment activities for monitoring or network visibility infrastructure;
- Strong knowledge of security telemetry collection, event correlation, threat detection, and threat hunting concepts. Very good communication and analytical skills;
- Language proficiency in English: meet or exceed the NATO STANAG 6001 Level 3 "Professional Proficiency";
- Relevant certifications in cyber security, such as Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP) or GIAC Security.

Desirable:

- Experience designing large-scale security monitoring and network visibility architectures;
- Experience integrating security monitoring tools with SIEM and SOAR tooling;
- Experience with automation, scripting, or orchestration;
- Experience supporting major platform upgrades, migrations, refreshes, or service transition activities;
- Prior experience in working in an international environment comprising both military and civilian elements;
- Knowledge of NATO responsibilities and organizational structure, including ACO and ACT.

Specific Working Conditions:

The contractor may be required to travel to NCIA locations in support of operational duties. In such cases the contractor will be reimbursed for travel costs according to NATO regulations for traveling on NATO duty. Contractors traveling for work purposes shall initiate travel requests from their designated duty station only. Travel within the duty country is considered commuting. If working from a remote location, the contractor shall provide IT equipment for the processing of public and unclassified information in support of their duties, including the capability to participate in video meetings using Microsoft based collaboration tools.

Required Level of Security Clearance:
NATO SECRET.