



JOB DESCRIPTION
Senior Engineer (Cyber Security Operations)
NATO Cyber Security Centre – Operations Branch
Grade: **G17**

This is a position within the NATO Communications and Information Agency (NCIA), an organization of the North Atlantic Treaty Organization (NATO).

To strengthen the Alliance through connecting its forces, the NCI Agency delivers secure, coherent, cost effective and interoperable communications and information systems in support of consultation, command & control and enabling intelligence, surveillance and reconnaissance capabilities, for NATO, where and when required. It includes IT support to the Alliances' business processes (to include provision of IT shared services) to the NATO HQ, the Command Structure and NATO Agencies.

The NATO Cyber Security Centre (NCSC) is responsible for planning and executing all lifecycle management activities for cyber security. In executing this responsibility, NCSC provides specialist cyber security-related services covering the spectrum of scientific, technical, acquisition, operations, maintenance, and sustainment support, throughout the lifecycle of NATO Communications and Information Systems (CIS). The NCSC enables secure conduct of the Alliance's operations and business in the context of NATO's C4ISR. The NCSC provides cyber security services to NCI Agency customers and users, as well as to all other elements of the Agency; this includes all Service Lines, Programme Offices, CIS Support Units/Elements, and the Agency Ops Centre. The NCSC is responsible for providing the broad spectrum of services in the following specialist security areas: CIS Security, Cyber Defence, Information Assurance, Computer Security and Communications Security. In executing its responsibilities, the NCSC provides support to the development and implementation of cyber security-related policy, strategy, and provides lifecycle security risk management services for all NATO CIS. The NCSC leads in the development of new capabilities and innovation in cyber security. The NCSC incorporates and provides specialist services to prevent, detect, respond to and recover from cyber security incidents.

The Operations Branch monitors, detects, analyses and responds to cyber incidents and cyber threat activity. It acts as the NATO Computer Emergency Response Team (CERT) for NATO with a NATO-wide mandate. It is responsible for sharing information related to cyber security incidents with NATO Nations and NCIA industry partners.

The Incident Analysis and Response Section (IA&R) delivers cyber incident, violation security investigation. The Section is responsible for delivering an efficient and effective response aiming at containing, analysing and removing the threat, coordinating the restoration of the affected services and sharing relevant information with the NATO bodies, NATO nations and the other NATO partners within the agreed frameworks. The Section ensures a timely reporting of security incidents to establish and maintain situational awareness across the Alliance's operational, cyber defence and security communities. Advanced digital, network, computer forensics and malware reverse-engineering capabilities are provided to support all phases of security incident detection and response to support post-incident analysis or as technical support to subsequent security investigations.

Duties:

Under the direction of Section Head, Incident Analysis and Response, the incumbent will perform duties such as the following:

- Provide technical and expert support for to the 24/7 Cyber Security Incident Analysis and Response processes, during normal working hours and on-call duties, including weekends and holidays;
- Lead or support a Cyber Security Response/Threat Hunting Team covering one or multiple physical locations, including NATO Alliance Operations and Missions;
- Plan and execute both static and dynamic code and Malware analyses/reverse-engineering and capture the results in a report which covers the technical aspects as well as the "so what?" for the decision makers and executives;

- Plan and execute complex and distributed Digital Forensic Analyses in the form of mobile (mostly on Apple iOS), network, system and memory forensics and capture the results in a report which covers the technical aspects as well as the “so what?” for the decision makers and executives;
- Develop and Maintain the Digital/Network Forensics and Malware/code analysis capabilities on deployable kits to support Cyber Incident Response and Threat Hunting;
- Develop tools, scripting, automation and integrations to automate activities as much as possible, mostly using Python and PowerShell;
- Identify and Share technical Indicators of Compromise with the other NATO stakeholders, the NATO nations and our different partners, in accordance with our sharing agreements;
- Write and review Standard Operating Procedures covering all aspects of Digital Forensics and Malware Analysis;
- Support CS OPS service delivery in the context of NCIA Enterprise Service Delivery Model and NCIA Customer Funded regime;
- Contribute to and standardise the information knowledge management of IA&R section and CS OPS Branch;
- Deputizes for higher grade staff when necessary;
- Performs any other duties as may be required.

Essential Experience and Education:

- A minimum requirement of a Bachelor's degree at a nationally recognised/certified University in a related discipline and 3 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 10 years extensive and progressive expertise in duties related to the function of the post;
- At least 3 years demonstrable experience in conducting Digital Forensics and/or Malware Reverse-Engineering or Analysis;
- Very good oral and written communications skills and reporting experience with capacity to communicate to different types of audience (senior executive, middle management, technical and non-technical);
- Very good abilities to lead a team of technical experts in adverse conditions;
- Very good understanding of the inner working of modern Operating Systems on Windows and Linux environment;
- Very good understanding of communication mechanisms on modern internet-facing systems: REST, SOAP, AJAX, MIME, API calls;
- Very good understanding of modern scripting languages: Python, PowerShell, JavaScript;
- Very good understanding of the TCP/IP stack up to the Application Layer;
- Good understanding of low-level programming language (assembly code) for Intel architecture.

Desirable Experience and Education:

- Master's Degree in IT or CIS security related discipline;
- Experience in conducting Digital Forensics and/or Malware Reverse-Engineering or Analysis on mobile devices;
- Experience in conducting Digital Forensics and/or Malware Reverse-Engineering or Analysis on Docker applications;
- Good understanding of the inner working of mobile Operating Systems (Android and iOS);
- Understanding of inner working of Industrial Control Systems (ICS);
- Good understanding of the MITRE ATT&CK framework and its applicability in Cyber;
- Hold relevant certifications such as SANS GIAC Forensics Analyst or Malware Reverse-Engineer;
- Good understanding of the management of CIS Service Delivery, ideally following ITIL framework;
- Prior experience of working in an international environment comprising both military and civilian elements;
- Knowledge of NATO responsibilities and organizational, including ACO and ACT.

Language Proficiency:

- A thorough knowledge of one of the two NATO languages, both written and spoken, is essential and some knowledge of the other desirable.
- **NOTE:** Most of the work of the NCI Agency is conducted in the English language.

Competencies or Personal Attributes:

- Deciding and Initiating Action: Takes responsibility for actions, projects and people; takes initiative and works under own direction; initiates and generates activity and introduces changes into work processes; makes quick, clear decisions which may include tough choices or considered risks.
- Delivering Results and Meeting Customer Expectations: Focuses on customer needs and satisfaction; sets high standards for quality and quantity; monitors and maintains quality and productivity; works in a systematic, methodical and orderly way; consistently achieves project goals.
- Relating and Networking - Easily establishes good relationships with customers and staff; relates well to people at all levels; builds wide and effective networks of contacts; uses humour appropriately to bring warmth to relationships with others.
- Adapting and Responding to Change: Adapts to changing circumstances; tolerates ambiguity; accepts new ideas and change initiatives; adapts interpersonal style to suit different people or situations; shows an interest in new experiences.