

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 Cyber Security Operations Branch mission is to monitor, detect, analyze and respond 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, Allies, NCIA industry partners and other stakeholders.

The CS Monitoring and Detection (M&D) Section delivers the 24/7 monitoring of crypto devices, networks, websites and email traffic to detect and identify incidents and threats. Supporting activities include the analysis of all-source cyber intelligence, indicators and warnings, coupled with internal security event sources to optimize NATO sensors enabling the earliest detection of security incidents. The Section hosts the NATO Cyber Security Helpdesk, which provides NCIA customers and stakeholders the single point of contact for cyber security related incidents and requests. It is the NATO 24/7 Point of Contact with NATO Nations for any cyber security incident related issues. As such, the section is the focal point for the sharing of technical information with Allies and other approved entities.

Network Monitoring and Incident Detection Cell (NMIDC) is responsible for 24/7 monitoring of NATO and NATO supported networks in order to identify, analyse and mitigate security threats. The cell performs the initial triage of security events and delivers technical assessments in addition to continuously improving the accuracy and efficiency of the detection capability through regular tuning and sensor optimisation. To achieve this, the cell utilises both internal and external resources along with cyber threat intelligence. Other supporting activities include maintenance of the NCIA Identified Malware Blacklist to ensure it remains relevant, and that known threats are published in accordingly.

Duties:

Under the direction of the Cell Head but mainly under own initiative, as a dedicated Threat Hunting Analyst the incumbent will work alongside a team of Security Analysts to proactively detect cyber security attacks against NATO networks. The role will involve researching and reacting to the latest threats, using industry leading tools to discover new and ongoing attacks in addition to the following main responsibilities:

- Provide subject matter expertise supporting the end-to-end threat hunting process;
- Develop hypotheses to be used in a threat hunt;
- Create security tool content such as searches, reports and dashboards to facilitate threat hunting;
- Perform in-depth analysis of suspicious activity to deliver conclusions and recommendations;
- Review and develop logging configurations to enable a comprehensive threat hunting capability;
- Develop and document threat hunting procedures;
- Share the results of threat hunts via presentations and technical reports;
- Propose possible optimisations and enhancements which help to maintain and improve NATO's Cyber Security posture;
- Implement peer review analysis and security reports as requested;
- Train and mentor team members on technical subjects;
- Produce Standard Operating Procedures covering all aspects of monitoring and detection activities;
- Support project activities in their area of responsibility when requested;
- Deputize for higher grade staff, if required;
- Perform 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;
- Comprehensive knowledge of the principles of Computer and Communication Security, networking, and the vulnerabilities of modern operating systems and applications acquired through a blend of academic or professional training coupled with practical professional experience;
- Knowledge and experience in analysis of various threat actor groups, attack patterns and tactics, techniques, and procedures (TTPs), deep analysis of threats across the enterprise by combining security rules, content, policy and relevant datasets;
- Knowledge of the TaHiTI threat hunting methodology and the MITRE ATT&CK framework;
- Strong analytical and problem-solving abilities, ability to identify patterns, detect anomalies and make accurate, informed decisions;
- Experience in performing in-depth cyber security analysis in large, complex networks using security use cases, relevant datasets, and documentation;
- Expertise in at least three of the following areas and a high level of experience in several of the other areas:
 - Cyber security threat hunting;
 - Security Incidents Event Management products (SIEM) – e.g. Splunk;
 - Splunk Processing Language;
 - Network Based Intrusion Detection Systems (NIDS);
 - Host Based Intrusion Detection Systems (HIDS);
 - Endpoint Detection and Response tools and their telemetry;
 - Sysmon configuration, Windows, and Linux log analysis;
 - Full Packet Capture systems – e.g. Nixsun, RSA/NetWitness;
 - Data visualisation and statistical analysis;
 - Computer security tools (Vulnerability Assessment, Anti-virus, Protocol Analysis, Anti-Virus, Protocol Analysis, Anti-Spyware, etc...);

- Proficiency in Intrusion/Incident Detection and Handling;
- Very good communications skills and reporting experience with capacity to communicate to different types of audience (senior executive, middle management, technical and non-technical).

Desirable Experience and Education:

- Industry leading certification in the area of cyber security such as, but not limited to: GCFA, GCIA, GNFA, GCIH;
- Experience writing detection rules for various systems, preferably in vendor-agnostic formats (e.g. Yara, sigma);
- Knowledge and experience in Splunk Enterprise Security suite;
- A good understanding of Security, Orchestrations, Automation and Response (SOAR) concepts and their benefits to the protection of CIS infrastructures;
- Knowledge and experience in threat hunting in corporate/government level environment;
- Strong knowledge of malware families and attack vectors;
- Ability to analyse attack vectors against a particular system to determine attack surface;
- Ability to produce contextual attack models applied to a scenario and propose methods for detection;
- A solid understanding of Information Security Practices relating to the Confidentiality, Integrity and Availability of information (CIA triad);
- Very good knowledge of potential security event sources and their interpretation and analysis in support of the incident detection and handling processes;
- Hands on experience on monitoring cloud services;
- Proven level of expertise in network traffic analysis;
- Proven level of expertise in malware analysis;
- Prior experience of working in an international environment comprising both military and civilian elements;
- Knowledge of NATO responsibilities and organization, 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.
- Achieving Personal Work Goals and Objectives - Accepts and tackles demanding goals with enthusiasm; works hard and puts in longer hours when it is necessary; seeks progression to roles of increased responsibility and influence; identifies own development needs and makes use of developmental or training opportunities.
- 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.