26589 - Detection Engineer

Location: Mons, Belgium.

Period: 395 (start on 26 Oct. 2026)

Deadline: 16 Sep. 2026

Duties/Roles:

- Design, develop, and maintain detection rules, alerts, and analytics across SIEM, EDR/XDR, NDR, and Cloud Security Tools;
- Implement detection logic using relevant languages (Sigma, SPL and KQL);
- Develop detections aligned with adversary behaviours and MITRE ATT&CK framework, focusing on Advanced Persistent Threats (APTs) targeting NATO alliance;
- Develop detections from available threat intelligence, participate in purple teaming events within NCSC and evaluate recommendations from Threat Hunting Team;
- Maintain and improve a structured detection engineering lifecycle established in CSOC, including: Design, Development, Testing, Deployment, Monitoring, Improvement and Review phases;
- Support CSOC efforts in improving Detection-as-Code practices and version control for detection content;
- Review and improve existing detection quality metrics established in CSOC;
- Conduct detection coverage assessments across monitored on- premise and cloud-based NATO infrastructure, in order to perform gap analysis against Adversary TTPs relevant to NATO infrastructure;
- Support CSOC threat modelling efforts in order to determine where detection capabilities should be improved;
- Define priorities for new detections based on the NATO attack surface, known risks, current trends and available intelligence;
- Collaboration with other Sections within NCSC and Defend Branch;
- Support incident handling team (CSIRT) by developing new detections based on newly released reports about vulnerabilities affecting NATO enterprise and information gathered during CSIRT`s operations;
- Collaborate with Threat Hunting Team (CTIS) to operationalize their findings into automated detections where applicable;

- Support the design of detection strategies for new technologies, platforms, and network architectures which could be introduced to CSOC, through various NATO projects;

- Review newly-ingested log data to ensure it aligns with the Splunk Common Information Model (CIM); carry out periodic audits, verify field extractions and event-type mappings, and liaise with data-source owners to resolve any inconsistencies or gaps;

- Provide security analysis and investigative support during ongoing cybersecurity incidents;

- Perform other duties as required, including ad-hoc projects, special investigations or support activities that fall outside the listed responsibilities, to ensure the overall effectiveness and resilience of the CSOC and NCSC.

Skills, Knowledge, Experience Required:

Mandatory:

- The candidate must have a currently active NATO SECRET security clearance;

- A minimum requirement of a Bachelor's degree from a nationally recognised/certified university in a related discipline and three years post-related experience. Alternatively, the lack of a university degree may be compensated by the demonstration of a candidate's particular abilities or experience of interest to the NCI Agency, provided the candidate has at least five years of extensive and progressive expertise in duties related to the function of the post;

- Minimum three years of hands-on experience in a Security Operations Centre (SOC, CSOC, GSOC or equivalent) or a closely related cyber monitoring environment;

- At least three years of experience designing, developing and maintaining detection rules, alerts and analytics across SIEM, EDR/XDR and cloud security tools (e.g., Splunk, Microsoft Sentinel, Azure, AWS);

- Experience translating attacker tactics, techniques, and procedures (TTPs) and threat intelligence into operational detection logic;

- Experience in analysis of raw telemetry and log data across multiple sources to identify detection opportunities and improve detection logic;

- Experience working with security monitoring and detection platforms such as Splunk, Microsoft Sentinel, Microsoft Defender XDR, Suricata, Snort, or comparable technologies;

- Experience working with log ingestion pipelines, normalization, and parsing processes used in security monitoring platforms;

- Adept at extracting, normalising and interrogating raw log data from diverse sources (e.g., Windows Event Logs, Linux syslog, Sysmon,

EDR/XDR platforms such as Microsoft Defender, Sentinel One, or CrowdStrike) using SIEM and query tools (Splunk, Microsoft Sentinel, Elastic Kibana). Able to filter, correlate and visualise events to verify alerts, reconstruct attacker activity across hosts, and provide actionable evidence for escalation and remediation decision;

- Hands-on packet-capture (PCAP) analysis experience – extracting, filtering and interpreting network traffic with tools such as Wireshark, tcpdump or Zeek to corroborate alerts, reconstruct attack timelines and support escalation decisions;

- Experience developing detections for network and edge security devices such as Cisco, Fortinet/Fortigate, Palo Alto, or comparable platforms;

- Experience supporting or mentoring less-experienced analysts and engineers, providing constructive feedback on investigation quality and reporting standards;

- Proven track record of conducting in-depth analysis of complex cyber-security incidents and delivering clear reports and recommendations to supporting teams and external partners;

- Strong written and verbal communication skills;

- Language proficiency in English: meet or exceed the NATO STANAG 6001 Level 3 "Professional Proficiency";

- Relevant cyber-security certifications (e.g., CISSP, CISM, GIAC-certified credentials such as GCIH, GCFA, or GSEC; CompTIA CySA+) or equivalent recognised professional training.

Desirable:

- A university degree (Bachelor's) in Cyber Security, Information Technology, Computer Science or a related discipline;

- Experience working in a regulated, high control environment such as defence, government, financial services or other enterprise sectors.

- Practical experience with automation or SOAR use cases, identifying repetitive manual tasks and creating enrichment or workflow improvements;

- Experience in working for or supporting a military or governmental organization.

Specific Working Conditions:

- 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.