26590 - Second Line Security Event Analyst

Location: Mons, Belgium.

Period: 395 (start on 26 Oct. 2026)

Deadline: 15 Sep. 2026

Duties/Roles:

- Review and validate investigations, supporting First-Line Analysts to ensure that alert closures, escalations, supporting evidence and investigation notes meet CSOC quality standards, confirming completeness, accuracy and procedural compliance;

- Act as the technical escalation point for cyber-security monitoring. Perform in-depth log analysis and threat-triage using the SIEM and SOAR platforms (Splunk Enterprise Security, Splunk SOAR, Microsoft Sentinel) together with supporting data sources and security appliances, and decide whether to forward the case to Incident-Handling Officers;

- Provide on-call support as part of a 24 × 7 roster, delivering round-the-clock coverage for second-line escalations;

- Design, develop, test and maintain detection rules, alerts and analytics across the cyber-security monitoring tool-set;

- Continuously adjust logic, thresholds, allow-lists, suppression rules and severity mappings to reduce false positives and improve coverage of emerging threats;

- Provide regular, constructive feedback and coaching to First-Line Analysts on investigation techniques, analytical approach and reporting quality, and support the onboarding and training of new staff;

- Support the Duty Second-Line Analyst with weekly operational responsibilities, monitor open tasks, follow up on pending actions and highlight issues that could affect CSOC service continuity;

- Participate in purple teaming events within NCSC in order to test and improve CSOC’s detection coverage;

- Collaborate with Threat Hunting Team (CTIS) to operationalize their findings into automated detections where applicable;

- Contribute to continuous-service-improvement initiatives by identifying workflow inefficiencies, monitoring blind-spots and recommending process enhancements;

- Write and update operational documentation, SOPs, run-books and knowledge-base articles that underpin Service Delivery Management (SDM) and the wider CSOC team;

- Represent the CSOC during project planning, implementation and transition activities, ensuring that monitoring and visibility requirements are fully considered, and offer expertise on detection-content design, log-source integration and security-tool configuration for any cyber-security projects undertaken by the organisation;

- Collaborate with internal and external stakeholders, working closely with other Defend-branch sections and, when required, the wider NCI Agency;

- 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.

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;

- Proven expert-level track record of conducting in-depth analysis of complex cyber-security incidents and producing clear, authoritative reports and recommendations for supporting teams and external partners;

- 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;

- Demonstrable ability to translate attacker TTPs and threat intel into operational detection logic and to conduct structured quality or peer reviews of analyst investigations, identifying gaps and recommending improvements;

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

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

- Strong written and verbal communication skills, with a history of producing clear investigation notes, escalation summaries and documentation;

- Very good communication and analytical 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;

- Hands on experience with cloud native security monitoring (Azure, AWS) and hybrid environments;

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

- 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.