26591 - Splunk Engineer

Location: Mons, Belgium.

Period: 395 (start on 02 Nov. 2026)

Deadline: 21 Sep. 2026

Duties/Roles:

- Act as one of the main engineers and Subject Matter Expert (SME) for SIEM and Log collection services within the Cyber Security Data team;

- As the SME, you will provide advice and technical assistance to other stakeholders, maintain technical expertise, awareness, and developments in related new technologies, and provide technical contributions to any projects related to the data security systems;

- Be responsible for management and further development of the data security systems;

- The contractor may occasionally be required to provide on-call support and intervene in the event of an issue to ensure the continued operational availability of the SIEM monitoring infrastructure;

- Following ITIL standards, provide support to Operations and Service Delivery management covering all stages of the data security systems lifecycle (e.g. Service Design, Transition, Operations, Change Management and Continual Service Improvement);

- Ensure that data security systems are installed, configured, and operating correctly and in line with dependencies with others systems or applications required;

- Ensure that all system components are continuously monitored and take appropriate technical and non-technical actions for solving detected issues;

- Ensure that data security systems operate within any KPI's, as defined in Service Level Agreements with NCSC customers. Support integration with external tools and any associated activities;

- Proactively identify and propose system improvements to ensure an up-to-date and stable environment;

- Justify business needs, prepare documentation and implementation plan for the Change Management Board. Implement the approved changes following co-ordination with other stakeholders;

- Coordinate with service delivery managers, end users and other stakeholders in support of related services; communicate with other NATO entities as well as industry partners where required;

- Develop and maintain documentation guidelines, standard operating procedures, system and service design documents and other relevant documentation that support management of the data security systems;

- Create technical and/or executive level reports as required; organise and deliver presentations and briefings for various audience up to NATO executive level;

- Perform 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 from a nationally recognised/certified university in a related discipline and two 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.

- At least 1 year of extensive practical experience as SIEM administrator with Splunk in large enterprise environment (deployment, installation, configuration and maintenance).

- Hands-on experience in the design and maintenance of distributed Splunk architectures.

- At least 2 years and expert level experience related to SIEM and Log collection management activities.

- Demonstrable experience of analysing and interpreting system, security and application logs in order to diagnose faults and spot abnormal behaviours.

- Practical hands-on experience in systems and tools administration, especially Linux environment;

- Comprehensive knowledge of the principles of computer and communication security, networking, and the vulnerabilities of modern operating systems and applications.

- Practical skills in writing Bash, Python or Ansible scripts to support repetitive tasks automation;

- Solid Linux system and application administration and troubleshooting skills.

- Solid understanding of regular expressions.

- Ability to develop clear and concise technical documentation, including procedures.

- Good communication abilities, both written and verbal, with the ability to clearly and successfully articulate complex issues to a variety of audiences and teams.

- Very good communication and analytical skills.

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

- Possessing industry leading certification in the area of Cyber Security such as CISSP, CISM, CISA, GSNA, and SANS GIAC.

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;

- Extensive practical experience (as system administrator) with Splunk Enterprise security, Splunk SOAR and Splunk UBA;

- Practical experience with Git software;

- Hands-on experience with Ansible as an automation technology;

- Experience in creation/modification of custom parsers;

- Software engineering including programming and/or scripting knowledge (python, shell scripting, PowerShell);

- Prior experience automating interactions between systems using APIs;

- A solid understanding of Information Security Practices; relating to the Confidentiality, Integrity and Availability of information (CIA triad.);

- ITIL Service Management certifications;

- Experience in developing Splunk Applications;

- Content management experience in Splunk, especially Enterprise Security and Advanced Search and Reporting;

- Hands-on experience with network infrastructure and virtualized environments;

- Previous experience working for Cyber Security related organisations (CERTs, security offices);

- Experience with log collection in cloud environment such as Azure or AWS;

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

Specific Working Conditions:

Normal working hours 08:30-17:30. On-call duties after working hours, on weekends or holidays are required.

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.

The incumbent may require to work on 12 hours pattern during weekdays but not exceeding an average of 38h per week In case of an enterprise-level Cyber Incident, the incumbent may be required to work extended hours and on shifts, including nights and weekends, to provide a 24/7 Cyber Incident Response.

Required Level of Security Clearance:

NATO SECRET.