26595 - Cyber Security Guard and Diode Engineer

Location: Mons Belgium.

Period: 395 (start on 19 Oct. 2026)

Deadline: 18 Sep. 2026

Duties/Roles:

1. Central system administration and configuration of Guards and Data Diodes to ensure continuing functionality and availability;

a. Hardware and software systems installation and configuration;

b. Implementation and verification of guards and data diode configuration to meet customer cross-domain data exchange requirements;

c. Adaptation of release markings and/or email attachment types;

d. configuration of additional cross-domain flows;

e. User and access management;

f. Monitor system performance and availability;

g. Analyze, troubleshoot and resolve application issues;

h. Development of automation scripts to meet day to day system administration tasks.

2. Updating of Guard and Data Diode software/patches

a. Monitor patch releases;

b. Test new software and patches;

c. Support A2SL process for approval of software updates;

d. installation and configuration of software and patch updates.

3. Documentation of Guards and Data Diode systems

a. Development of SOPs and other documentation for repetitiveactivities;

b. Produce and maintain comprehensive documentation for all implemented systems.

4. Operational support of Guards and Data Diodes

a. Technical support in troubleshooting infrastructure and operational issues;

b. Collaboration with other teams for a successful resolution;

c. Provide technical support and guidance by answering end-user requests to identify issues in secure cross-domain data exchange.

Skills, Knowledge, Experience Required:

- NATO Secret security clearance;
- At least 3 years practical experience in cyber security or related field.
- Extensive knowledge and experience (min 3 years) in the following areas:
- Linux System Administration (preferred RedHat Enterprise Linux).
- Scripting/Automation (Bash, Python, Ansible).
- Other Boundaries Protections Devices such as firewalls.
- System security, including hardening and SELinux.
- System monitoring and troubleshooting.
- Experience with network protocols and traffic analysis.
- Ability to troubleshoot complex network security issues.
- LAN/WAN networking including protocol network architecture.
- TCP/IP protocols and services.
- Strong stakeholder management skills – can demonstrate evidence of developing and maintaining strong and effective relationships with internal stakeholders at all levels in an organization.
- Flexible and adaptable; able to work in ambiguous situations.
- Very good communication and analytical skills.

Training/certifications:

- Relevant certifications in cyber security, such as Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP) or GIAC Security.

Desirable:

- Experience in working for or supporting a military or governmental organization.
- Understanding of Information Security Practices relating to the Confidentiality, Integrity and Availability of information (CIA triad.)

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 NCIA, that is, at least 10 years extensive and progressive expertise in duties related to those in this Statement of Work..

Required Level of Security Clearance:

NATO SECRET.