

26751 - Adversary Emulation Tool Management Support Service

Location: Mons, Belgium.

Period: 91 (start on 07 Dec. 2026)

Deadline: 05 Nov. 2026

Duties/Roles:

1) System administration, monitoring and reporting:

- Install, configure, update Linux operating systems;
- Manage user accounts, permissions and security;
- Configure network service (DNS, DHCP, NFS, SSH);
- Proactively review logs and alerts to identify any technical issues, errors, or failures in the monitoring process;
- Produce and distribute reports related to system health, monitoring activities, and compliance status (e.g., audit logs, system performance metrics);
- Daily: Verify the system is healthy (Check CPU, memory, disk usage, etc.), if not resolve the issues to make system up and running;
- Daily: Review logs for errors or anomalies;
- Daily: Respond quickly to outages or system alerts;
- Daily: Check ITSM and take an action for requests, changes and incidents.

2) System Documentation:

- Document configuration and changes: Keep up-to-date documentation of all configurations, integration steps, troubleshooting procedures, and system maintenance tasks;
- Maintain an inventory: Keep track of all integrated identity sources, IAM systems, and external tools;
- Weekly: Do the maintenance (Schedule and apply updates, check system resources, etc.);
- Weekly: Periodically test backup restores to ensure data integrity;
- Weekly: Identify and resolve performance bottlenecks or capacity issues.

3) Automation and Scripting

- Improve system efficiency: Identify areas where automation could reduce manual intervention and improve operational efficiency;
- Monthly: Analyse trends in resource usage and plan for upgrades;
- Monthly: Ensure service levels are met; report to stakeholders;

- Monthly: Verify and update hardware/software inventory.

Skills, Knowledge, Experience Required:

Mandatory:

- The candidate must have a currently active NATO SECRET security clearance;
- Bachelor's degree in Computer Science, Information Technology, or related field or at least 6 years of experience;
- 3+ years of relevant experience in IT security, with a focus on System Administration, Security Tools Management in large organisations;
- Relevant and proven experience acquired during the 3+ years time:
- Linux Systems administration(Install/configure/maintain Linux based servers, apply system updates/patches, monitor system performance/logs, manage users/permissions/settings of the platform);
- Docker management (maintain Docker containers, troubleshoot Docker based applications and volumes);
- Strong understanding of security best practices;
- IP switching and routing, experience in network troubleshooting;
- Virtual Infrastructure understanding based on VMWare technologies;
- Good engineering skills including programming and/or scripting knowledge (python, shell scripting, PowerShell);
- Demonstrable experience of analysing and interpreting logs in order to diagnose faults and spot abnormal behaviours;
- Experience in Proxy management (Configure/maintain proxy, implement routing rules/access control);
- A good understanding of NATO organization and its IT infrastructure;
- A good understanding of Service Management, monitoring and reporting tools, such as Solarwinds;
- A good understanding of ITIL Service Management;
- A good understanding of system instrumentation solutions such as Ansible;
- Certifications such as CISSP, CISM, or CISA, or equivalent;
- A good understanding of an international environment comprising both military and civilian elements.

Required Level of Security Clearance:

NATO SECRET.