26588 - DFIR Tool Engineer

Location: Mons, Belgium.

Period: 395 (start on 26 Oct. 2026)

Deadline: 16 Sep. 2026

Duties/Roles:

- Deploy, configure, monitor, troubleshoot and maintain the suite of digital forensics and XDR tools, ensuring all systems are kept up to date in accordance with IT Service Management (ITSM) processes;

- Integrate user feedback and implement enhancements to improve usability and effectiveness, which may include developing automation scripts or custom configurations to meet operational requirements;

- Work onsite, at SHAPE, Mons, Belgium, for coordination purposes and due to the accesses required;

- Support change management processes to deliver & maintain tools and capabilities from the section;

- Execute coordination and information gathering activities within NCSC, NCIA, and with other NATO & external stakeholders, in support of the above activities.

Skills, Knowledge, Experience Required:

Mandatory:

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

- 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;

- At least 5 years of experience in deploying, managing and maintaining forensics and XDR tools in complex environments;

- At least 2 years of experience with remote acquisition tooling (Fidelis and/or F-Response) with demonstrated ability to configure, support deployment at scale including resolving failed collections and performance issues;

- At least 2 years of experience with collaboration tools such as Jira and Confluence;

- Strong understanding of forensically sound acquisition principles (integrity verification, repeatability, minimizing system impact);

- Windows Server/Desktop administration skills: services, drivers, certificates, event logs, permissions, remote management;

- Ability to diagnose host-level issues impacting forensic tools (resource contention, disk I/O, endpoint controls, OS patch impacts);

- Experience with Red Hat Linux and managing a fleet of servers with Ansible;

- Experience working with vendors (support tickets, log bundles, upgrades) and communicating impacts/ETAs to investigators/analysts;

- Experience implementing least-privilege access, credential handling, and audit logging for forensic systems;

- Knowledge and demonstrable experience with scripting languages and integration tools including PowerShell, Python, Bash, Batch and Ansible;

- Very good communication and analytical skills;

- Good understanding of cyber security concepts;

- Good understanding of network communication protocols;

- Have an in-depth understanding of infrastructure concepts related to Hosting, Networks, IP address Management, firewalls, certificates, Load balancing and Proxy;

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

- Ability to produce detailed technical documentation and follow change management processes;

- Relevant certifications in cyber security, GIAC (Global Information Assurance Certification) or equivalent.

Desirable:

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

- Experience in working for or supporting a large company with complex and heterogenous environments;

- Experience in delivering forensics tools support and finding innovative solutions;

- Professional experience in digital forensic analysis;

- Experience with Microsoft Azure, Microsoft Defender for Endpoint.

Specific Working Conditions:

Normal working hours 0830-1730, with the exception of working non-standard working hours up to 360 hours annually to support incidents and on-call activities.

Required Level of Security Clearance:

NATO SECRET.