26587 - MISP Senior Engineer

Location: Mons, Belgium.

Period: 395 (start on 19 Oct. 2026)

Deadline: 14 Sep. 2026

Duties/Roles:

System administration:

- Proactively manage and maintain multiple servers running the MISP software ensuring the necessary confidentiality, integrity and availability of the tool and information;

- Stand up, configure and manage dedicated MISP instances in support of NATO exercises;

- Regularly update MISP software to the latest version and support test and validation efforts for change management processes;

- Configure and extend the system monitoring of MISP installations;

- Maintain the ansible playbooks related to MISP setup and configuration;

- Maintain and improve documentation related to MISP installations within NATO;

- Act as a subject matter expertise for NATO MISP communities, providing community members with guidance on MISP deployment architectures and their benefits and limitations.

Content Management:

- Develop and maintain (python) scripts to automate and integrate MISP with other subsystems within NATO such as the SIEM, IDS, etc;

- Support quality management efforts by creating and maintaining content quality rules;

User and Community Management:

- Provide support to the user-community of NATO managed MISP instances;

- Provide feedback to the user-community on regular basis, and on daily-basis during exercises;

- (Depending on the need, and the skills of the individual): During exercises, lead a team of multiple MISP Operators to support information flow, quality control and user management;

- Support the streamlining and automation of user management process with a combination of IT Service Management tools (ITSM) and Identity and Access Management (IDAM) tools e.g. Cerebrate or Keycloak.

MISP Training support

- Plans for, prepares and delivers online MISP training;
- Support the preparation of individual training packages to validate training objectives have been met.

Coordination

- Coordinates the work of a small group of engineers.

Skills, Knowledge, Experience Required:

Mandatory:

- The candidate must have a currently active NATO 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 10 years practical experience in architecting deployment solutions;
- At least 10 years practical experience in coordinating the work of a small group of engineers;
- At least 10 years practical experience in system administration with LAMP servers - Linux, Apache, MySQL/MariaDB, PHP;
- At least 10 years practical experience in configuration of web applications;
- At least 10 years practical experience in Python scripting;
- At least 10 years practical experience in MVC software development and code review of web applications mostly in PHP and SQL;
- Good understanding of cyber security principles, best practices, concepts and technologies;
- Ability to work independently and in a team, including the ability to monitor and support a team;
- Excellent organization, communication and analytical skills;
- Very good technical understanding of the cyber threats to web-based products;
- Language proficiency in English: meet or exceed the NATO STANAG 6001 Level 3 "Professional Proficiency".

Desirable:

- Experience as sysadmin of a MISP Threat Sharing platform;

- Experience developing code (python, PHP) for MISP;
- Experience with RedHat;
- RHCSA certification or similar;
- Experience working with open-source communities;
- Experience in multinational cyber exercises e.g. Locked Shields, Crossed Swords, Cyber Coalition, etc;
- Experience with CakePHP.

Specific Working Conditions:

The contractor may be permitted to perform work remotely, from a different NATO nation than the duty location, for up to a maximum of twenty percent (20%) of their total working time, subject to prior approval by their NCIA designated Resource Manager. 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.