

26755 - Cyber Threat Intelligence Researcher

Location: Brussels, Belgium.

Period: 1596 (start on 18 Jan. 2027)

Deadline: 12 Nov. 2026

Duties/Roles:

The Contractor will be responsible for conducting cloud engineering to support NATO's cyber threat intelligence production. The Contractor must:

- Use the CTAB Cyber Threat Intelligence Platform and other sources to conduct research into prioritized cyber threat actors to discover new infrastructure and capabilities under the direction of the team lead.
- Conduct pattern analysis on threat actor infrastructure to detect new malicious infrastructure, and script and automate that detection to allow for threat intelligence at scale.
- Find and analyse potential new cyber threats to NATO based on existing or novel techniques and scripts, and correlate with all available sources to establish an adequate threat picture.
- Translate threat actor tactics, techniques and procedures into actionable intelligence for 1) network defenders through creating detection signatures, contextualizing IoC's, and writing standardized CTI products, and 2) strategic cyber analysts for use in intelligence production to decision makers.
- Support other threat researchers in their activities, and advise and assist strategic cyber threat analysts in understanding complex technical topics.
- Participate in team and branch calls as required by the team lead to give status updates on projects and developments pertinent to the Contractor's tasks, and ensure constant delivery of findings, mostly comprising indicators of compromise and MITRE techniques, on novel threat actors.
- Equally deliver scripts and methodologies that improve on current processes and tooling and enhance NATO's ability to track adversaries in cyberspace.

Skills, Knowledge, Experience Required:

Mandatory:

- All general and domain specific qualification requirements stated in the AAS+ Framework Agreement shall be applicable (e.g., required English proficiency);

The Contractor will require a NATO SECRET clearance.

- In addition to the generic qualification requirements established in the AAS+ Agreement, The Contractor must have:

- A university degree from a nationally recognised/certified university in a quantitative discipline (Computer Science, Engineering, Statistics, Operations Research, etc.) with substantial computer science content and 2 years of specific experience – OR - at least 4 years' experience similar to the tasks described in this SoW and relevant industry recognized certificates;

- Knowledge and experience in analysis of various threat actor groups, attack patterns and tactics, techniques, and procedures (TTPs) to produce actionable threat intelligence to enable network and host defences in organizations with demonstrable impact;

- Experience with and knowledge of the intelligence lifecycle, analytical tradecraft and frameworks such as MITRE ATT&CK;

- Good communication skills, both orally and written. Able to translate complex technical topics into information conveyable to non-domain experts. Can easily cooperate with other threat researchers by taking and giving feedback;

- Knowledge of network and system fundamentals and experience in any of the following cybersecurity fields: network monitoring, threat hunting, incident response, red teaming, host/network forensics, or reverse engineering;

- Experience with programming in scripting languages such as Python.

Required Level of Security Clearance:

NATO SECRET.