26756 - Cloud Engineer

Location: Brussels, Belgium.

Period: 1596 (start on 18 Jan. 2027)

Deadline: 12 Nov. 2026

Duties/Roles:

- Under the guidance and supervision of the NATO IS Procurement Service, the selected service provider will be responsible for the execution of the tasks and for the delivery of the specialist products specified in this SOW.

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

- Ensure the availability, confidentiality, and integrity of CTAB's cloud environment, and do so in a cost-effective way, by provisioning, configuring and monitoring cloud resources using Terraform and ensure all code and work is maintainable and documented.

- Work with data scientists, software engineers, researchers and end-users to translate their requirements into functionalities within the cloud environment, while ensuring security is front-and-centre.

- 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.

- The Contractor shall produce the Deliverables as specified in the task order management under supervision of the NATO Project Manager. The Contractor shall submit Deliverables to the NATO Project Manager for Quality Review, test or inspection not later than the dates specified by the NATO Project Manager.

- The Contractor shall continuously validate any deliverables with the NATO Project Manager and peers within CTAB.

- The Contractor shall hold periodic sessions with the NATO Project Manager to make sure that the deliverables are aligned with NATO's expectations.

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 systems engineering 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 of and experience in maintaining and developing multi-account AWS cloud environments, specifically in core AWS products such as Lambda, S3, CloudTrail, ECS, EC2, and similar, as well as working according to industry best practices such as AWS's Well Architected Framework;

- Significant experience in using Terraform to build and maintain cloud infrastructure as code, setting up CI/CD pipelines, automating containerized workloads on ECS and conditional access;

- Able to set up monitoring, logging and alerting with tools like CloudTrail and GuardDuty, and experienced in managing IAM with SSO, VPC networking, and least-privilege security controls;

- Proficient in Python and Bash and knowledge of Docker, Linux administration and Git;

- Experience within cybersecurity and/or the intelligence domain is strongly preferred but not required for this role, as is experience with Azure;

- Good communication skills, both orally and written;

- Able to translate complex technical topics into information conveyable to non-domain experts;

- Can easily cooperate with non-cloud experts and explain conducted work, as well as give and take feedback and create clear and structured documentation based on the work conducted.

Required Level of Security Clearance:

NATO SECRET.