DevSecOps Engineer

Axient Systems B.V., Delft

About us

At Axient Systems, we are shaping the future of sovereign space capability. Based in Delft, at the heart of the Dutch aerospace ecosystem, we develop advanced satellite systems that support critical commercial and government missions. Our solutions enable secure communications, defence, security, and resilient infrastructure where performance and reliability are essential.

As a growing and ambitious organisation, we offer professionals the opportunity to contribute directly to innovative space projects that make a real impact on society, security, and technological progress.

We are looking for a DevSecOps engineer who builds and runs the pipelines and infrastructure our software teams deploy on, so that security is engineered in rather than bolted on.

The role

You own the CI/CD pipelines, the deployment infrastructure and the secure build and release chain for our ground software, including delivery onto classified and restricted networks. Today our developers make this work themselves; a dedicated engineer frees that time for software development and gives us the security depth the programme demands.

What you will do

- Design, build and maintain compliant CI/CD pipelines for our ground software.
- Implement infrastructure as code in air-gapped and disconnected environments.
- Manage container orchestration and secure deployment on Kubernetes.
- Integrate security scanning, vulnerability management and software supply chain verification into the pipeline.
- Maintain on-premises artefact repositories with strict access control, and manage secrets on restricted networks without internet access.
- Deploy and maintain applications on classified and restricted networks, within the accreditation the environment requires.
- Set up monitoring and logging, and help the software teams build to the deployment and security constraints from the start.
- Work with the security officer on the controls and evidence the accreditation of the environment needs.

You own the pipeline and the deployment infrastructure; our ground software architect owns the software architecture, and our security officer owns the accreditation of our environments. The three of you work together daily.

What you bring

- Degree in computer science, software engineering or comparable, or equivalent experience.

- 5+ years in DevOps or DevSecOps, with demonstrable ownership of CI/CD pipelines for secure or restricted environments.
- Infrastructure as code (Terraform, Ansible) and container orchestration (Kubernetes, OpenShift, Docker).
- Strong Linux system administration, including hardened distributions.
- Scripting in Python, Bash or similar.
- Hands-on experience applying security standards such as NIST 800-53, and the judgement to know which control matters where.
- Professional working proficiency in English; Dutch is an advantage.

Desirable

- Deploying and maintaining software on restricted, air-gapped or classified networks.
- Software supply chain security: SBOM, dependency scanning, artefact signing.
- On-premises artefact repositories (Artifactory, Nexus) and secrets management (HashiCorp Vault or similar).
- Monitoring and logging stacks (ELK, Splunk, Grafana).
- Security certifications.
- Defence or other government-contracting experience, and its audit and accreditation demands.

What we offer

- A role where you build the foundation the whole software organisation deploys on, from the ground up.
- Competitive, market-aligned salary and benefits, real ownership of your discipline, and room to grow as the organisation scales.
- On-site work in Delft, limited hybrid working possible.

Particularities

This role requires Dutch security screening. You will need a VOG (Certificate of Conduct) to start, which is quick to obtain and lets you begin work on the project immediately.

You might also need a VGB-B clearance. This takes longer, and we support you through it. It is required for some aspects of the role, so you must be eligible for it and willing to undergo the screening, but you do not need to have it in hand to join us.

Interested?

Apply via the vacancy on LinkedIn or the registration form on our website.

In your application, include a short description of one CI/CD pipeline or deployment you owned for a secure or restricted environment: the constraint that shaped it, one thing that went wrong, and what you changed. Applications without this description will not be reviewed.