

26727 - Senior Engineer (DevSecOps)

Location: Brunssum, the Netherlands.

Period: 270 (start on 07 Dec. 2026)

Deadline: 02 Nov. 2026

Duties/Roles:

- Progress against agreed project plans, milestones, and deliverables;
- Status of design, integration, configuration, testing, deployment, and migration activities;
- Achievement of key project objectives and technical deliverables;
- Identification of project risks, issues, dependencies, and proposed mitigation actions;
- Summary of completed activities during the reporting period;
- Planned activities and milestones for the upcoming reporting period;
- Status of technical documentation, design artefacts, and acceptance deliverables;
- Quality assurance activities performed and any identified non-conformities;
- Resource utilisation and effort expended against assigned tasks, where required;
- Escalations, decisions, or support required from NCIA stakeholders.

Skills, Knowledge, Experience Required:

Mandatory:

- The candidate must have a currently active NATO SECRET security clearance;
- Bachelors degree in Computer Science, Software Engineering, Information Technology, Cybersecurity, Engineering or a related discipline or an equivalent combination of education and professional experience;
- 5 years experience in DevSecOps, DevOps, software engineering, platform engineering or infrastructure automation roles;
- Experience supporting on-premises CIS environments, including enterprise data centres, mission-critical infrastructure and operational systems;
- Experience designing, implementing and maintaining DevSecOps pipelines and automation frameworks in secure, on-premises environments;

- Experience integrating security controls and compliance requirements throughout the software development lifecycle (SDLC);
- Experience supporting containerized and cloud-native technologies deployed in on-premises environments;
- Experience implementing Infrastructure as Code (IaC), configuration management and automated deployment solutions;
- Experience working within military, defence, government or mission-critical operational environments is desirable;
- Experience producing technical documentation, deployment procedures, architecture diagrams, security artefacts and operational handover documentation;

Expertise/experience in several of the following areas:

- DevSecOps and CI/CD: Designing, implementing and maintaining Continuous Integration and Continuous Delivery/Deployment (CI/CD) pipelines;
- DevSecOps principles and practices, including secure software delivery and automated security testing;
- CI/CD platforms such as GitLab, Jenkins, Azure DevOps or equivalent;
- Integrating automated build, testing, deployment and security validation processes;
- Infrastructure as Code and Automation: Developing and maintaining Infrastructure as Code (IaC) solutions;
- Tools such as Terraform, Ansible, Puppet or equivalent. Automating infrastructure provisioning, configuration management and deployment processes;
- Scripting and automation using Python, Bash, PowerShell or similar;
- Containerization and Platform Technologies: Deploying and supporting containerized applications and services;
- Container technologies such as Docker and orchestration platforms such as Kubernetes;
- Container security, image management and container lifecycle management;
- Platform engineering concepts and modern application deployment architectures;

- Cybersecurity and Secure Development: Integrating security controls throughout the software development lifecycle;
- Secure coding practices, application security principles and software assurance methodologies;
- Implementing Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Software Composition Analysis (SCA) and vulnerability management processes. Implementing secrets management, identity and access management and secure configuration practices;
- Systems and Infrastructure: Supporting Linux and Windows Server environments;
- Virtualization platforms and enterprise infrastructure technologies;
- Supporting application hosting platforms, middleware, databases and supporting infrastructure services;
- Monitoring, Logging and Observability: Implementing monitoring, logging and observability solutions;
- Tools such as Prometheus, Grafana, Elastic or equivalent monitoring platforms;
- Performance monitoring, incident response, troubleshooting and operational reporting.

Certifications

- The proposed contractor shall possess at least one of the following certifications:
- Certified Kubernetes Administrator (CKA);
- HashiCorp Certified: Terraform Associate;
- Docker Certified Associate (DCA);
- Equivalent industry-recognized DevOps, platform engineering or automation certification.

In addition, the contractor shall possess at least one cybersecurity-related certification:

- CompTIA Security+;
- GIAC Security Essentials (GSEC);
- ISC2 Certified in Cybersecurity (CC);
- Equivalent industry-recognized cybersecurity certificate.

Required Level of Security Clearance:

NATO SECRET.