We are looking for an experienced **DevSecOps Engineer** to drive end-to-end software supply chain security and enterprise CI/CD platform engineering across a cloud-native Kubernetes ecosystem on Google Cloud Platform (GCP). In this role, you will bridge software engineering and platform security, championing DevSecOps practices, engineering advanced Jenkins Groovy and Tekton pipelines, and securing artifact delivery using tools like SonarQube, Sonatype IQ, and SLSA frameworks.

If you bring a strong software engineering background, deep expertise in Kubernetes and CI/CD automation, and a passion for building resilient, highly secure release platforms, we want to hear from you.

DevSecOps Engineer

Nr ref.: 85/10/2026/MD/270837/jobs.pl Kraków (małopolskie)

What you can expect from us?

- Contract: B2B
- Work-Life Balance & Flexibility: Hybrid work model (3 days per week in our modern Kraków office, combining team collaboration with remote flexibility)
- Global Exposure: Opportunity to work in a dynamic, international environment with cutting-edge open-source and cloud technologies

Employment agency entry number 47

this job offer is intended for people over 18 years of age

What will your tasks involve?

- **CI/CD Platform Engineering:** Design and expand Jenkins Groovy Shared Libraries and modern Kubernetes-native Tekton pipelines
- **Software Supply Chain Security:** Integrate security scanning tools (SonarQube, Sonatype IQ) and implement security frameworks (SBOM/CycloneDX, SLSA, artifact signing)
- **Automation & Tooling:** Develop custom Python automation scripts for advanced configuration processing (JSON/YAML) and API integrations
- **Cloud & Deployment Support:** Publish and standardize Helm charts and Terraform modules for applications on Google Cloud Platform (GCP) and Kubernetes
- **Performance & Support:** Optimize CI/CD pipeline performance (caching, parallelization) and troubleshoot user-reported pipeline issues for engineering teams

What we expect from you?

Requirements (Must-Have):

- **Experience:** 7+ years of overall engineering experience, including at least 3 years specializing in CI/CD platform engineering or DevSecOps
- **Jenkins & Groovy:** Strong expertise in engineering advanced Jenkins Groovy Shared Libraries
- **Advanced Python:** Proven experience in building custom automation tools and scripts in Python (advanced JSON/YAML processing)
- **Packaging & Containerization:** Deep knowledge of package management (Maven, NPM, Python packaging) and hands-on exposure to Helm, Terraform, and container image metadata

- **Software Supply Chain Security:** Practical understanding of SLSA frameworks, SBOM (CycloneDX), and image digests
- **Security Scanning Tools:** Experience with SonarQube and Sonatype IQ for container scanning and SAST
- **Performance Optimization:** Proven track record in pipeline tuning (caching, parallelization, dependency pruning)
- **Compliance Awareness:** Strong awareness of security compliance and governance standard practices

Nice-to-Have:

- Artifact signing and attestations (Cosign, OCI registry standard)
- Publishing patterns for Terraform modules and Helm charts
- Experience with GitOps or release automation patterns
- Hands-on GCP or AWS cloud experience

Soft Skills:

- Precise and effective technical communicator
- Strong documentation discipline
- Ownership mindset with the ability to operate independently with minimal supervision