

## **DevSecOps Engineer**

Nicosia, Cyprus

### **About Rimes**

Rimes provides enterprise data management solutions to the global investment community. Driven by our passion for solving the most complex data problems, we provide our clients with investment intelligence that powers more than US\$75 trillion in assets under management annually. The world's leading institutional investors, asset managers and service providers rely on Rimes to help them make better investment decisions using accurate information and industry-leading technology.

### **The Opportunity**

The DevSecOps Engineer role has been created to embed security into our engineering, DevOps and cloud delivery pipelines. Working closely with our Development, DevOps, Infrastructure and Security teams, you will engineer, automate and maintain security controls across our CI/CD pipelines, cloud workloads and application lifecycle.

This position is critical in uplifting our secure by design practices, reducing vulnerabilities, and ensuring our rapidly evolving development environments adhere to best-in-class security standards. (Infosec presentations highlight the explicit gap for DevSecOps capability and security integration into Dev and Cloud projects).

### **Key Responsibilities**

- Integrate security controls into CI/CD pipelines (Azure DevOps, GitHub Actions, Jenkins or equivalent).
- Implement automated SAST, SCA, DAST, container scanning and secrets management controls. (Referenced in secure development lifecycle expectations.)
- Work with Development and DevOps teams to ensure secure design principles, threat modelling and secure coding practices are embedded early in the lifecycle.
- Engineer and maintain tooling for vulnerability management across code, containers, pipelines and cloud workloads.
- Automate security guardrails across Azure resources, Kubernetes clusters, API gateways, serverless workloads and service meshes.
- Support and enhance the deployment of security policies (IAM, key vaults, network controls, hardening baselines).
- Partner with engineering squads to review architecture changes and ensure security requirements are addressed.
- Contribute to incident response activities where application or pipeline security is implicated.
- Contribute to uplift of our secure engineering policies, developer training and SSDLC processes. (Supports expectations stated in internal assessments and training docs).

### **Requirements:**

- Experienced in DevOps or platform engineering with a strong security mindset.
- Hands-on experience with at least one CI/CD platform (Azure DevOps preferred).
- Good understanding of application security principles (OWASP Top 10, SANS/CWE Top 25).

- Experience integrating or running security scanners: SAST, SCA, DAST, container scanning, IaC scanning.
- Experience with infrastructure as code (Terraform, ARM/Bicep, Helm).
- Familiar with cloud security (preferably Azure) and container security best practices.
- Capable of supporting vulnerability management processes and remediation workflows.
- Ability to collaborate with Software Engineering, DevOps, SRE, Cloud and Security teams.
- Strong communicator able to translate risk into engineering friendly language.

**Nice to Have:**

- Kubernetes (AKS), service mesh, container runtime security.
- Experience integrating security telemetry into SIEM/SOAR pipelines.
- Exposure to Zero Trust design principles.
- Threat modelling and automated security testing frameworks.

*Only selected candidates will be contacted for interviews. We appreciate your understanding. Thank you for considering a career with us.*

Rimes is committed to promote the values of diversity and inclusion throughout the business. Whether it's through recruitment, retention, career progression or training and development, we are committed to improving opportunities for people regardless of their background or circumstances.

Visit our [Careers](#) page to see our complete listings.