

# DEVOPS ENGINEER

**Toulouse, Permanent contract, Full time, Starting date : ASAP**

## Delair

Delair is one of the world's most experienced provider of drone-based solutions combining its high performance, long range UAV hardware with sophisticated analytics technology and operational services. We enable enterprises to monitor and digitize their physical assets from the air and turn the collected data into valuable business insights. Our solutions are used globally by customers in industries such as utilities, construction, agriculture, transportation, mining and oil & gas.

By joining Delair, you will participate in what is broadly recognized as the biggest technological paradigm shift of our generation: the digitization of the physical world. The combination of drones, Cloud-based services, AI (Artificial Intelligence) and Machine Learning, makes Delair a pioneer and leader in shaping tomorrow's technology landscape.

It is in technical excellence and perpetual innovation process that we recognize ourselves.

This is why we encourage pioneering ideas and incent our teams to develop their creativity.

As a young, energetic and highly motivated team, we work in a stimulating and pleasant working environment. Dedication and innovation are rewarding and rewarded, giving you a unique opportunity to gain valuable and challenging experience in a rapidly growing business with passionate and easy-going enthusiastic people

Our cloud platform ingests large amounts of aerial images as raw material to produce maps, 3D models and business analysis. We work hard to provide our clients with powerful tools to access their data quickly and interact with them in real-time . Help us go further in this task.

## Job description

We are looking for a Devops Engineer for facilitating the continuous code deployment, automated resource provisioning and scaling, security control, monitoring & troubleshooting. This is a very hands-on position, highly visible for someone who wants to build and maintain innovative and scalable solutions using the latest open source technologies.

## Your missions

- Help maintaining a strong level of robustness, scalability, performance and security of the platform.
- Participate in design and architecture discussions.
- Lead the charge for resolving issues in our production, test and dev environments.
- Work closely and collaboratively with software engineering to deploy and operate our cloud processing pipeline.
- Build and maintain tools for deployment, monitoring and operations.
- Make application development and deployment easier for the engineering team.
- Ensure backend services, Web and API services are running with adequate provisioning for meet a predefined SLA.
- Ensure adequate security of the environment and all resources.
- Build tools and systems to manage security.
- Help implement Security Development Lifecycle in current development workflow.

## The Profile

We are looking for candidates with the following skills and experience:

- Proven working experience in driving effective implementation & adoption of Security Development Lifecycle (SDL) and software maturity model.
- You care about operational efficiency and can embrace a DevOps approach to cloud operations.
- Investigate new tools & technologies our team can use to solve problems for the business.
- You are open to the idea of working across the stack with a range of technologies, as opposed to wanting to focus on a specific area of engineering.
- You're not freaked out by the ambiguity common in a startup.
- You can operate effectively at a fast-paced company and embrace change.
- You're a self-starter.

We know it would be suspicious for you to master all these technologies but definitely let us know what you used among these things:

- Containers orchestration (Docker, Kubernetes, Swarm, Consul, Vault).
- IaaS Cloud Provider (AWS, Google Cloud, Azure).
- NoSQL Database (MongoDB, Elastic Search).
- Network stack.
- Building and maintaining automated continuous integration (GitlabCI, Travis) with automated testing.
- Knowledge of common security threats, such as attack techniques, evasive techniques, and preventative & defensive methods.
- Knowledge of common infrastructure security flaws, risks, and possible remediation.
- Coding and Scripting (Python, NodeJS, Go).
- Bash / Linux/Unix Administration.

