DevOps and MLOps Engineer

Job Type: Full-time

About the Role:

As an **DevOps and MLOps Engineer** at DOCEO AI, you will be responsible for deploying, monitoring, and maintaining machine learning models as well data ingestion pipelines, software pipelines (CI/CD) in pre-production and production environments and cloud infrastructure. You will work at the intersection of software development, data engineering and machine learning, ensuring our AI-driven insights are delivered efficiently and securely.

Responsibilities:

- Automate **software and infrastructure deployment**, ML model monitoring, retraining, and performance evaluation.
- Implement and manage **CI/CD pipelines** for software and machine learning workflows.
- Design and implement scalable **MLOps pipelines** for training, testing, and deploying models.
- Manage and optimize cloud-based **compute and storage infrastructure**.
- Establish comprehensive **monitoring**, **logging**, and **alerting** for data and model pipelines.
- Ensure compliance with **data security and governance** standards, including **role-based access, secrets management, and encryption.**
- Integrate **DevSecOps** practices into CI/CD pipelines, including automated vulnerability scans, container image scans, and secret management.
- Implement and maintain **network and application security controls** (IAM/RBAC, WAF, DDoS protection, intrusion detection, and monitoring) to improve platform reliability and scalability.
- Collaborate with AI researchers and full-stack engineers to support **continuous integration** of ML components.

Requirements:

- Bachelor's or master's degree in computer science or a related field.
- 2–5 years of relevant experience in MLOps, DevOps, or cloud engineering roles.
- Experience with **containerization and orchestration** tools, such as **Docker** and **Kubernetes or similar tools**.
- Experience in deploying production software on **major cloud platforms (Azure, AWS, GCP)**.

- Strong understanding of **reliability engineering practices** (HA architectures, disaster recovery, automated failover, backup strategies).
- Familiarity with **network security controls** (WAF, DDoS protection, VPCs, private subnets, firewalls).
- Experience with Infrastructure as Code (IaC) tools such as **Terraform.**
- Experience with CI/CD tools such as **Jenkins, GitLab CI, GitHub Actions, or similar tools.**
- Experience with **DevSecOps workflows** (automated vulnerability scanning, container image scanning, dependency security).
- Experience with **monitoring tools** for model drift and bias detection and **pipeline observability tools.**
- Cloud Certifications (**Azure, AWS, GCP**) will be considered an asset.
- Familiarity with **LLMOps** and LLM orchestration and pipelining tools, such as **LangChain**, **LLamaIndex**, and managing **Vector databases** will be considered an asset.

Work Schedule

- On-site presence required 5 days a week during standard business hours.

Eligibility Requirements

- Must be a Canadian citizen, permanent resident, or hold an existing valid work permit.

For job inquiries please email resume to hr@doceo.ai