AVALY.AI

JOB TITLE:

AI Security Engineer

Location: Remote (Global) or Hybrid (US/Canada preferred)
Commitment: Contract-to-hire or Full-time
Start Date: ASAP

Avaly.ai is building the next-generation platform for **AI observability, security, and compliance**, focusing on securing AI-first systems and protecting against adversarial attacks, regulatory violations, and model failures. Think **Wiz or Datadog for AI**, powered by open-source tools—not proprietary software.

Must-Have Skills & Experience

- **Hands-on experience with Python scripting** and automation for security/monitoring tasks.
- Experience deploying and working with tools like **Grafana, or Prometheus**
- Experience managing infrastructure using **Docker and Linux environments**
- Comfortable using or integrating with **cloud platforms (AWS/GCP/Azure)**
- Exposure to **Kubernetes** or building multi-tenant architectures
- Knowledge of **basic AI/ML lifecycle** (especially model evaluation & drift detection), **API security** and **data pipeline hardening**.

Nice-to-Have (Optional but Valuable)

- Experience deploying and working with tools like **MLflow, SIEM tools**, **HiddenLayerOTI**, or other threat intelligence platforms
- Familiarity with **AI Fairness 360** or other fairness/bias auditing tools
- Familiarity with **adversarial testing frameworks** like **ART (IBM)** or **Microsoft Counterfit**

Ready to shape the future of AI Security?

To apply, please include the job title you're applying for in the subject line of your email and attach your resume.

We also encourage you to include a short cover letter or personal note that highlights why you're passionate about securing intelligent systems and what makes you a strong candidate for the role. If available, feel free to share your GitHub profile, LinkedIn, or links to relevant projects. We're excited to hear from you!

Send an email to careers@avaly.ai