We are seeking an innovative Senior Software Engineer specializing in ML Ops for one of our clients, a globally recognized financial enterprise. This is a highly specialized role embedded within a pioneering cybersecurity initiative. You will bridge the gap between software engineering, data science, and security by developing solutions that evaluate Artificial Intelligence and Machine Learning models for cyber vulnerabilities and advanced threats.

Senior Software Engineer (ML Ops & AI Security)

Nr ref.: 41/9/2026/AS/270261/jobs.pl Warszawa (mazowieckie)

What you can expect from us?

- **Stable Employment:** A permanent employment contract providing stability within a highly regulated, global enterprise framework.
- **Hybrid Work Model:** A collaborative hybrid setup requiring 3 days a week from a modern office.
- **Cutting-Edge Innovation:** A unique opportunity to work at the intersection of AI and Cybersecurity, shaping how a global institution secures its machine learning assets.
- **Global Scope & Impact:** Play a critical role in a brand-new project that defines the future of AI risk management for thousands of internal systems.

Employment agency entry number 47

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

What will your tasks involve?

- **AI Security Evaluation:** Develop and own end-to-end software solutions designed to evaluate AI/ML models for potential cyber capabilities and security risks.
- **Benchmarking & Testing:** Set up, execute, and maintain benchmarking frameworks (utilizing tools such as DeepEval) to systematically determine the safety and output behavior of various models.
- **Cross-Functional Collaboration:** Interface directly with Model Risk Management and Data Science teams to align security assessments with enterprise AI governance.
- **Data Analysis & Engineering:** Leverage strong software engineering and data analysis skills to process evaluation outputs and generate actionable security insights.
- **Platform Integration:** Ensure that model evaluation tools and processes are seamlessly integrated into the broader enterprise cybersecurity platform.

What we expect from you?

- **Proven Expertise:** Solid background in software engineering combined with significant data science and ML Ops experience.
- **Model Evaluation:** Hands-on experience evaluating AI/ML model performance, behavior, and risk, ideally using evaluation frameworks like DeepEval.
- **Cybersecurity Awareness:** A strong understanding of cybersecurity concepts and the unique vulnerabilities associated with deploying machine learning models in production.

- **Analytical Skills:** Strong data analysis capabilities to interpret complex model outputs and benchmarking results.
- **Technical Stack:** Proficiency in programming languages relevant to AI/ML and backend systems (e.g., Python, Go, or Java), along with experience in deploying and testing models.