AI Security Intern [IDA: 00018]

Descrição da função

1.Analyze security risks in AI/ML systems (model, data, infrastructure)
2.Study and test AI-specific threats (e.g., adversarial attacks, data poisoning, model extraction, prompt injection)
3.Develop proof-of-concept attacks and corresponding defensive mechanisms
4.Build Python-based tools for AI security testing and automation
5.Perform security evaluation of AI pipelines (training, inference, API exposure)
6.Support secure AI architecture design and risk assessment activities

Requisitos

1.Strong programming skills in Python.
2.Experience with AI/ML frameworks such as TensorFlow, PyTorch, or Hugging Face.
3.Experience with Docker or DevSecOps tools
4.Familiarity with open-source AI models and their applications in security.
5.Familiarity with reinforcement learning or generative AI models.
6.Strong problem-solving skills and ability to work in a collaborative environment.

Identificação da vaga
REF7401M

Área funcional
Engineering

Local
Singapore

Pessoa jurídica
AUMOVIO Singapore Pte. Ltd.

O que oferecemos

Ready to take your career to the next level? The future of mobility isn't just anyone's job. Make it yours! **Join AUMOVIO. Own What's Next.**

Quem somos

Since its spin-off in September 2025 AUMOVIO continues the business of the former Continental group sector Automotive as an independent company. The technology and electronics company offers a wide-ranging portfolio that makes mobility safe, exciting, connected, and autonomous. This includes sensor solutions, displays, braking and comfort systems as well as comprehensive expertise in software, architecture platforms, and assistance systems for software-defined vehicles. In the fiscal year 2024 the business areas, which now belong to AUMOVIO, generated sales of 19.6 billion Euro. The company is headquartered in Frankfurt, Germany and has about 87.000 employees in more than 100 locations worldwide.