

MATV/S.

Machine Learning Lead (f/m/d)

**Job posted**

11.08.2026

**Two Openings**

Both identical,
both permanent

**Starting Date**

Immediately or
by arrangement

**Contract**

Permanent, full-
time, six-month
probation

**Location**

Tübingen, or
remote within
Germany

We secure AI agents. You will own the detection and analysis systems that decide what gets through.

About MATVIS

MATVIS secures AI agents. We inspect traffic inline, on any model and any infrastructure, and stop prompt injection, PII leakage, data exfiltration and shadow AI before they reach anything that matters. Model-agnostic, ISO 27001 certified, and deployed inside our customers' own environments so their data never leaves.

Founded in Tübingen in 2023. Enterprise customers run us in production today, most of them working against AI Act and NIS2 deadlines, so they can deploy AI with confidence.

Your Role

As one of our two Machine Learning Leads, you will:

- Own core detection and analysis features end to end: dataset collection, training, evaluation, deployment, and everything that breaks afterwards.
 - Work across the full threat surface: prompt injection, jailbreaks, PII detection and redaction, content filtering, data exfiltration, agent misuse.
 - Build the parts of the detection stack that are not models: traffic analysis for Policy Autopilot, parametrization, and the business logic that turns a signal into a decision.
 - Build and defend the benchmark harness. Detection rate, false positive rate and latency are product metrics here, and customers feel all three.
 - Design security into the pipeline itself. We build our detection infrastructure in house, from data provenance through to our own training and evaluation tooling.
 - Ship containerized services into Docker and Kubernetes environments.
 - Debug across the full stack, from model output through runtime, container and network.
-

Must have

- Full MLOps ownership. You have taken a model from raw data into production and kept it running.
- Strong Python and PyTorch.
- A security instinct: pentesting, red teaming, CTF, bug bounty or adversarial ML. If you can attack systems and train models, we are interested regardless of what your degree says.
- Benchmarking and evaluation discipline.
- Clear written communication and a collaborative, adaptable way of working. Small team, high async load.
- Docker and REST APIs.
- Fluent English, written and spoken.

Nice to have

- Experience attacking LLM applications that were already in production.
 - Kubernetes, SQL.
 - German.
-

What we offer

- Competitive salary based on industry standards.
 - Tübingen, in the middle of Cyber Valley, next to the Max Planck Institute, ELLIS and the Tübingen AI Center. Or remote within Germany.
 - Flexible working hours.
 - A team small enough that what you build ships within weeks.
-

Connect with Us and Apply Now!

Take the next step in your career and apply today. Send us your CV as a PDF to

career@matvis.com

with **Machine Learning Lead** in the subject line. No cover letter needed. If you have public work, such as CVEs, CTF write-ups, papers or repositories, send the links. They count for more than the CV. We read every application and reply either way.

MATVIS is committed to diversity and inclusion. We strive to build a diverse team and welcome applications from people of different backgrounds, skin color, religion, sexual identity, gender, disability or age. Follow us on LinkedIn to stay up to date with what's happening at MATVIS.