

AI & SYSTEMS

Hybrid AI Lab for Security and IT

Local and hosted models for technical research and development

Working project · validation planned

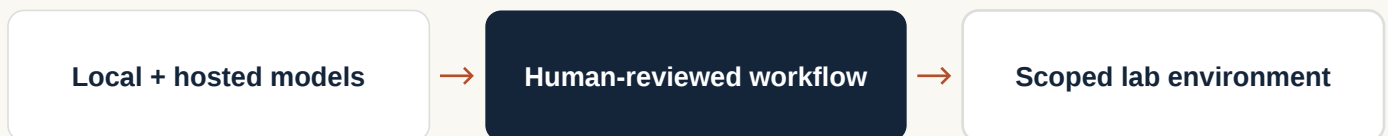
Personal project · ongoing

Deployed local language models and integrated hosted AI models for security research and IT workflows. Used AI-assisted development to create apps and websites, including this portfolio, and documented a broader lab design for repeatable technical work.

Project objective

Create a flexible environment for technical research, coding assistance, and troubleshooting. Local and hosted models provide different options, with the choice guided by the task, available resources, and the information involved.

Documented design



The guide connects model services with chat or development tools and a separate Linux lab environment. The full architecture and its controls are design work; end-to-end validation remains a next step.

Current work

01 Local model deployment

Set up local language models for hands-on use in technical research and IT workflows.

02 Hosted model integration

Combined local models with hosted AI services to support technical tasks and AI-assisted application and website development.

03 Lab documentation

The setup guide covers model services, user interfaces, development workflows, and a proposed virtualized security lab. It separates components and records the intended operating approach.

SKILLS & TOOLS

Local LLMs / Hosted model APIs / AI-assisted development / Virtualization design / Technical documentation

AI & SYSTEMS

Evidence, scope & next steps

Design choices and scope

The local-and-hosted workflow is in use. The broader security-lab architecture is documented; benchmark results and security-control validation are not yet included.

01 Deliberate model selection

Choose local or hosted processing based on the task and review what information would leave the local environment.

02 Human review of actions

Keep model suggestions separate from execution. Review generated code and proposed commands before using them in a scoped lab.

03 Separate lab resources

Design for dedicated lab targets, separate credentials, and recoverable virtual environments. Keep secrets out of shared documentation.

SCOPE & LIMITATIONS

The current scope is model deployment, integration, AI-assisted development, and documented lab design. Validation of environment isolation, model performance, and adversarial behavior remains future work.

What I learned

The value of the project is in connecting tools into a usable workflow and making the design understandable. Model output still needs review, testing, and clear documentation before it becomes a dependable technical result.

Next steps

1. Verify network boundaries and test virtual-machine snapshot recovery.
2. Validate credential separation and the information sent to hosted services.
3. Run a repeatable set of benign coding and IT tasks; document accuracy, latency, and required human corrections.