AI & SOVEREIGN CLOUD

Innovation and Compliance for regulated Industries

SPEAKERS

Markus M. Moeltner
Senior Consultant
Topic Lead AI
Spike Reply

Mobil: +49 170 6500123
Mail: m.moeltner@reply.de

Felix Jung
Consultant
Topic Lead Sovereign Cloud
Spike Reply

Mobil: +49 152 54911198
Mail: f.jung@reply.de

SAFETY AND RISK ASSESSMENT OF AI

OVERVIEW: SCOPES & DOMAINS

Consumer App

Company App

Pre-trained models

Optimized models

Self-trained models

used / purchased

built

Governance & Compliance

Legal & Privacy Policy

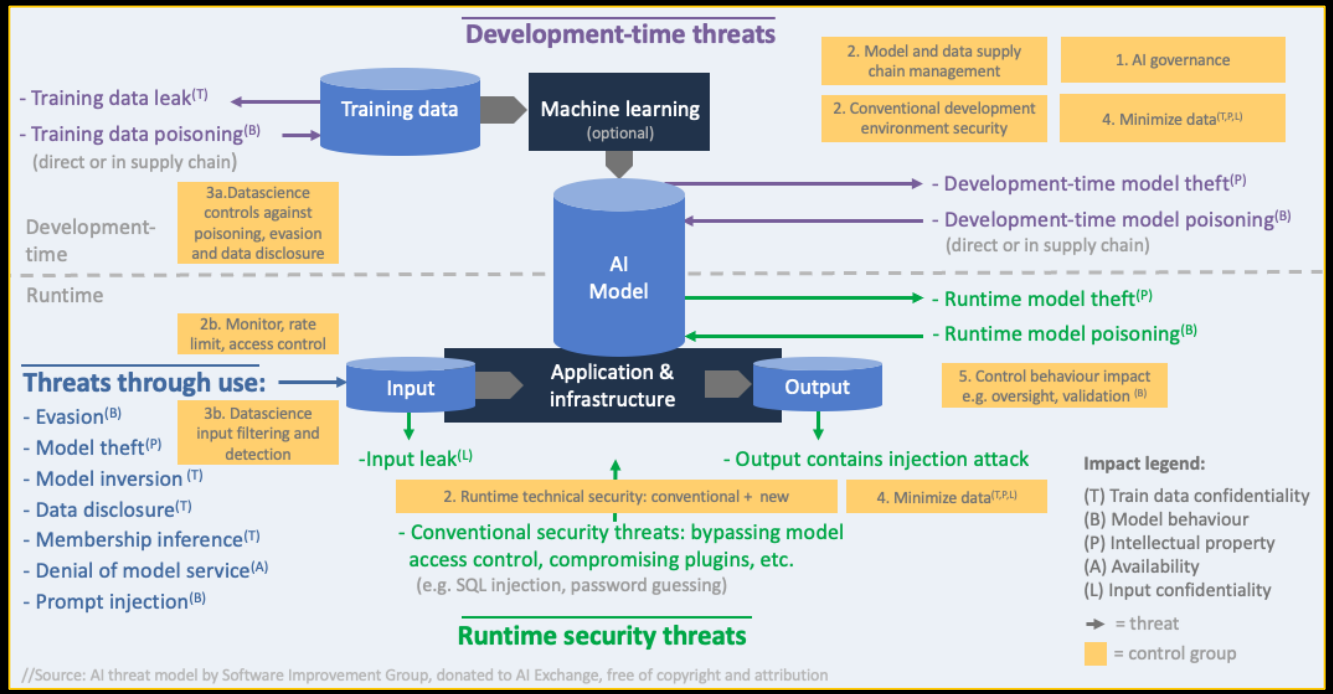
Risk Management

Controls

Resilience

THREAT MODEL

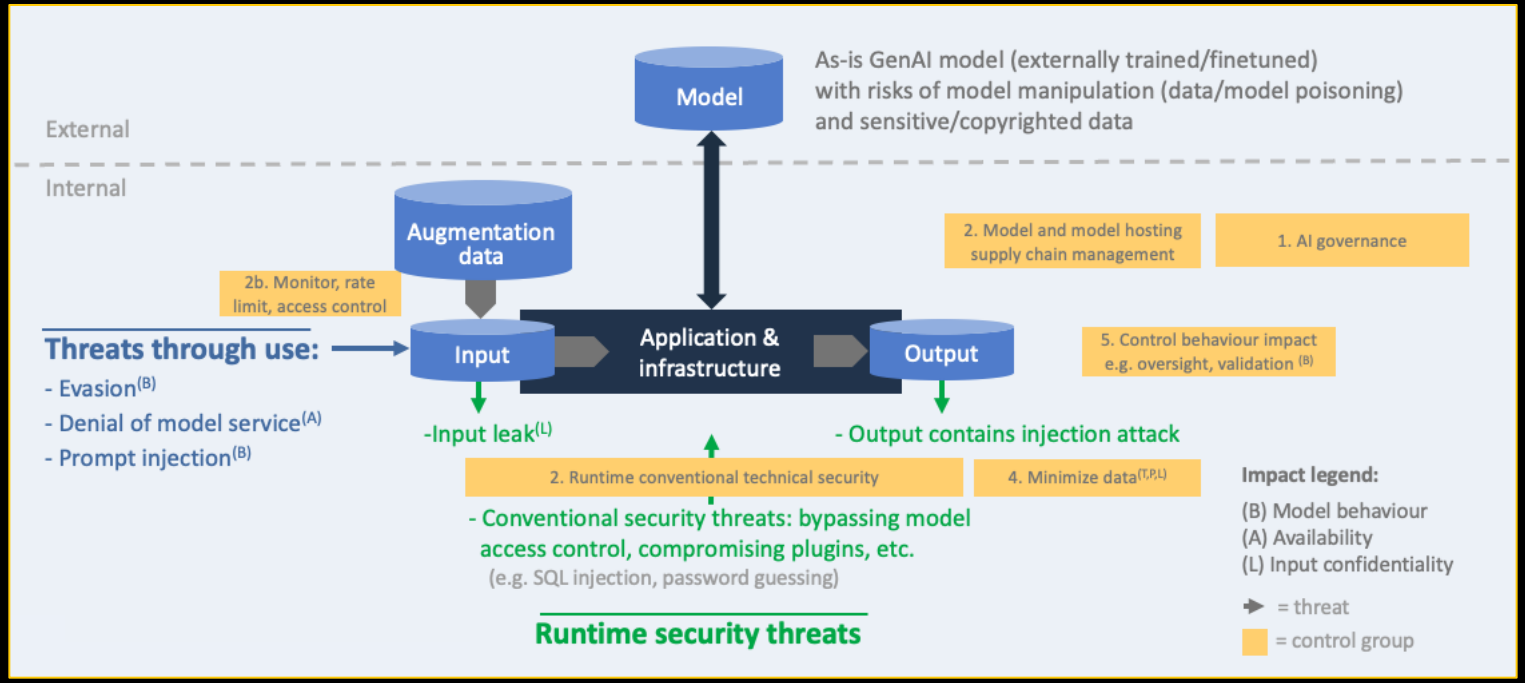
OPTIMIZED/ SELF-TRAINED MODELS



Source: owaspai.org

THREAT MODEL

PRE-TRAINED MODELS



Source: owaspai.org

SOVEREIGN CLOUD

MISCONCEPTION OF A SOVEREIGN CLOUD

Criteria:
Data, Metadata, Operations, Personnel, Control over Stack/Keys/Technologies, Jurisdiction under European law, Access Transparency and Traceability, …

MISCONCEPTION OF A SOVEREIGN CLOUD

Criteria:
Data, Metadata, Operations, Personnel, Control over Stack/Keys/Technologies, Jurisdiction under European law, Access Transparency and Traceability, …

Innovation
~~Less Sovereignty~~

Control
~~More Sovereignty~~

DIMENSIONS OF SOVEREIGNTY

Data Residency

- User, diagnostic, log and telemetry data remain in the compliance borders

→ No hidden data leaks into global systems

Operational Sovereignty

- Operation & support exclusively by local, verified personnel

→ No support and admin accesses by foreign specialists

Juridical Sovereignty

- Data only under EU/national law

→ No data release by the provider to legal requests from abroad

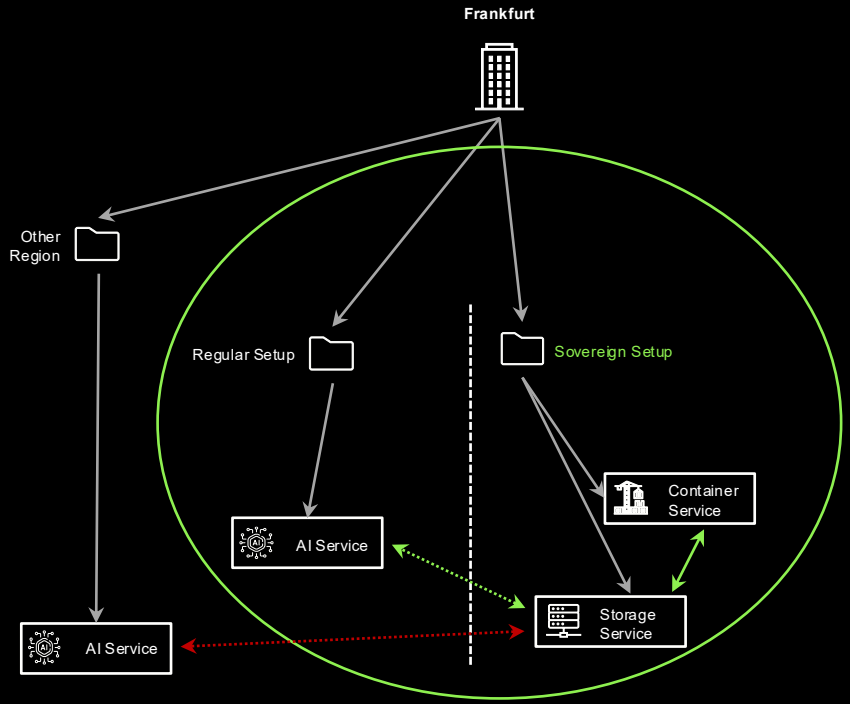
Software/System Sovereignty

- Control over technology stack & telemetry
- Partitioning between public and sovereign cloud

Transparency, Traceability, Auditability and deliberate control inside the legal sphere

SOLUTION APPROACH

CONTROLLED INFRASTRUCTURAL SEGMENTATION



SOVEREIGNTY IN THE SEGMENTED CLOUD ENVIRONMENT

Data Transfer

Pseudonymization prior to processing in the non-sovereign part

Encryption

Exclusive control over encryption keys (HYOK)

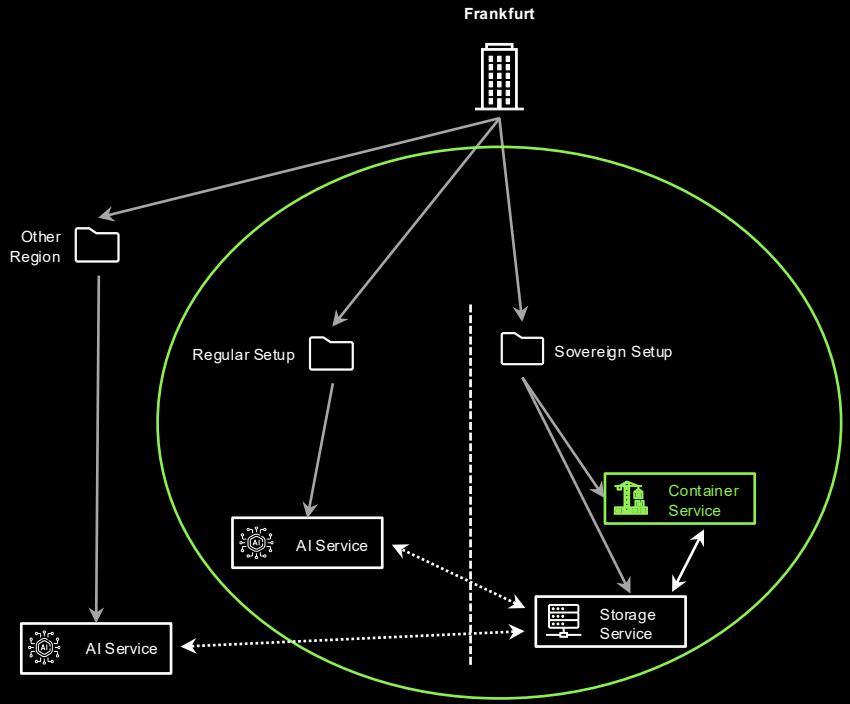
Backups

Resilient backups within the EU

Process transparency

Auditable recovery and complete traceability in the process

CONTROLLED INFRASTRUCTURAL SEGMENTATION



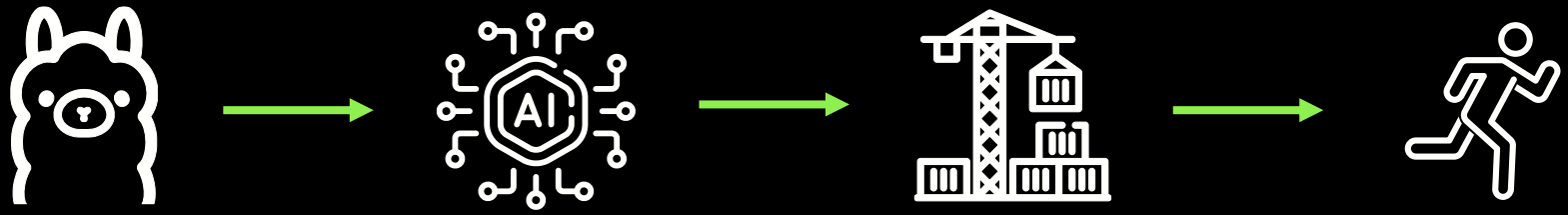
CONTAINERIZED AI

Open-source tool for executing locally installed AI models, e.g. Ollama, vLLM

Load open-source/ open-weight model, e.g. Mistral/ Llama/ Gemma models

Create a Dockerfile and build containers

Running containers on managed container platforms



BENEFITS FOR AI WORKLOADS

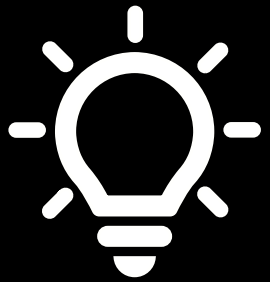
KEY TAKEAWAYS

AI security requires clear governance and compliance

When using AI, companies must establish clear rules, processes and controls to manage risks and comply with legal requirements.

Sovereignty means full control over data and operations

This includes complete control over the storage, processing and access of data, as well as ensuring that all processes and personnel comply with local/regional regulations.



Cloud-native AI services are available, but with limitations

Modern AI services in “sovereign” clouds are currently only available to a limited extent. The limitation is no longer in availability, but in the model selection and features.

Sovereign AI is possible with self-deployed models

Companies can achieve full control over AI applications by running their own models in isolated, self-managed environments – e.g., with open-source/open-weight models and container technologies.

THANK YOU
Q&A