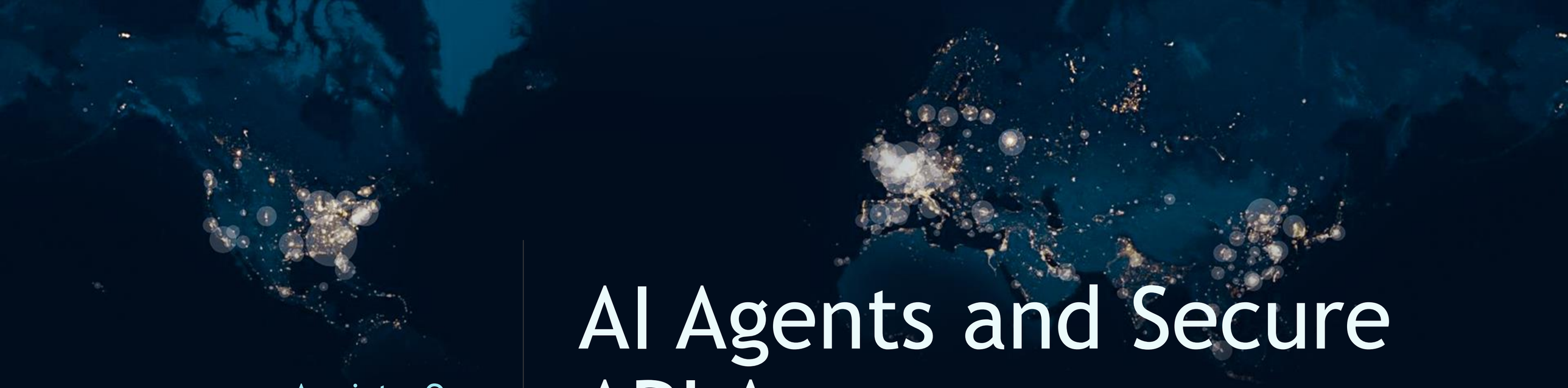


Aavista Oy
Merja Kajava

AI Agents and Secure API Access

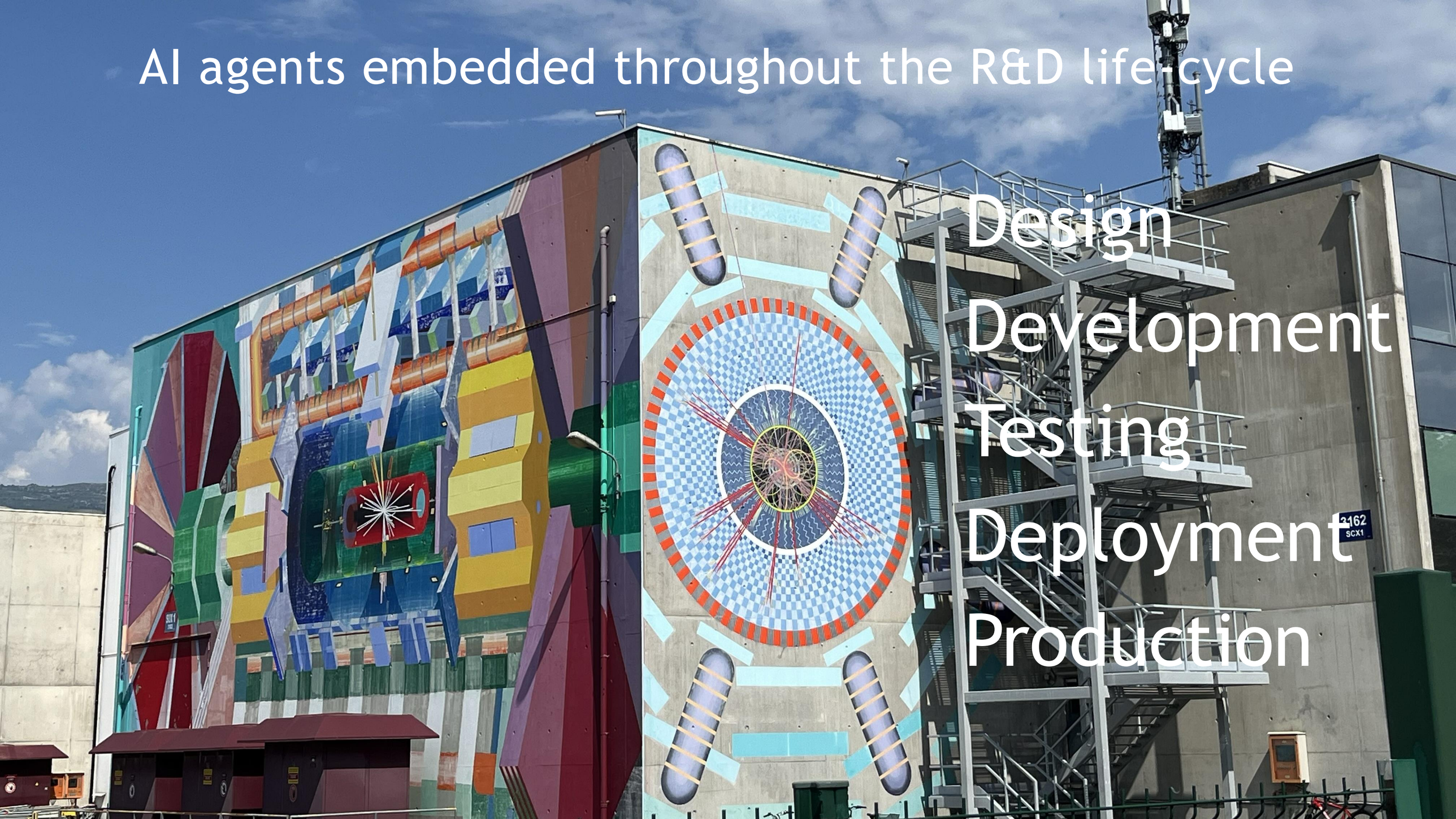
APIOps Helsinki 2026

AAVISTA

AAVISTA

Photo credit: NASA / Paul E. Alers

AI agents embedded throughout the R&D life-cycle



Design

Development

Testing

Deployment

Production

What are the elements of Agentic AI

Orchestration

Goals, profiles, skills

Model

Reason with goals

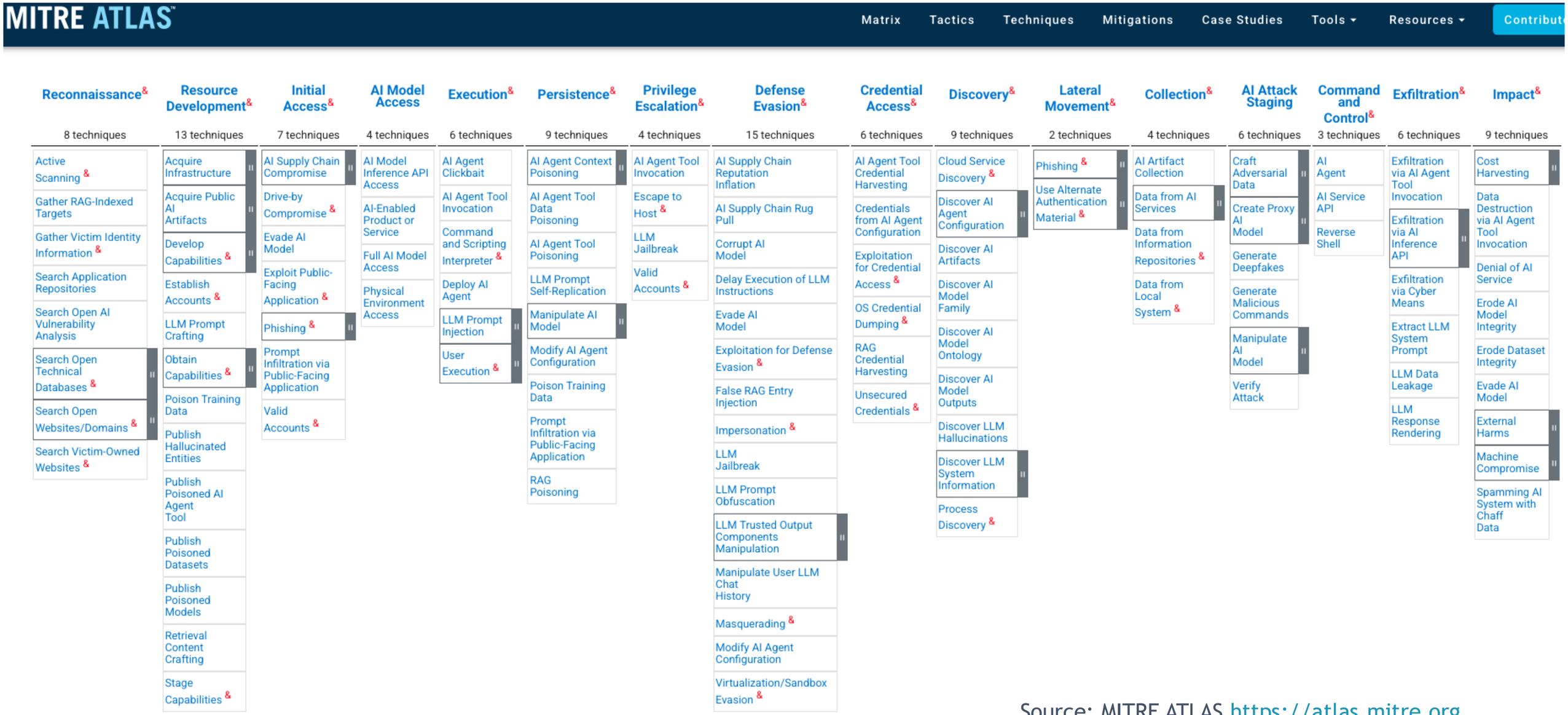
Tools

Integrate to data and 3rd party services and APIs

AAVISTA

AI agents as API consumers and API providers

Different types of threats are emerging



Source: MITRE ATLAS https://atlas.mitre.org

Compliance requirements are expanding

EU regulation, e.g.

- CRA
- DORA
- AI Act

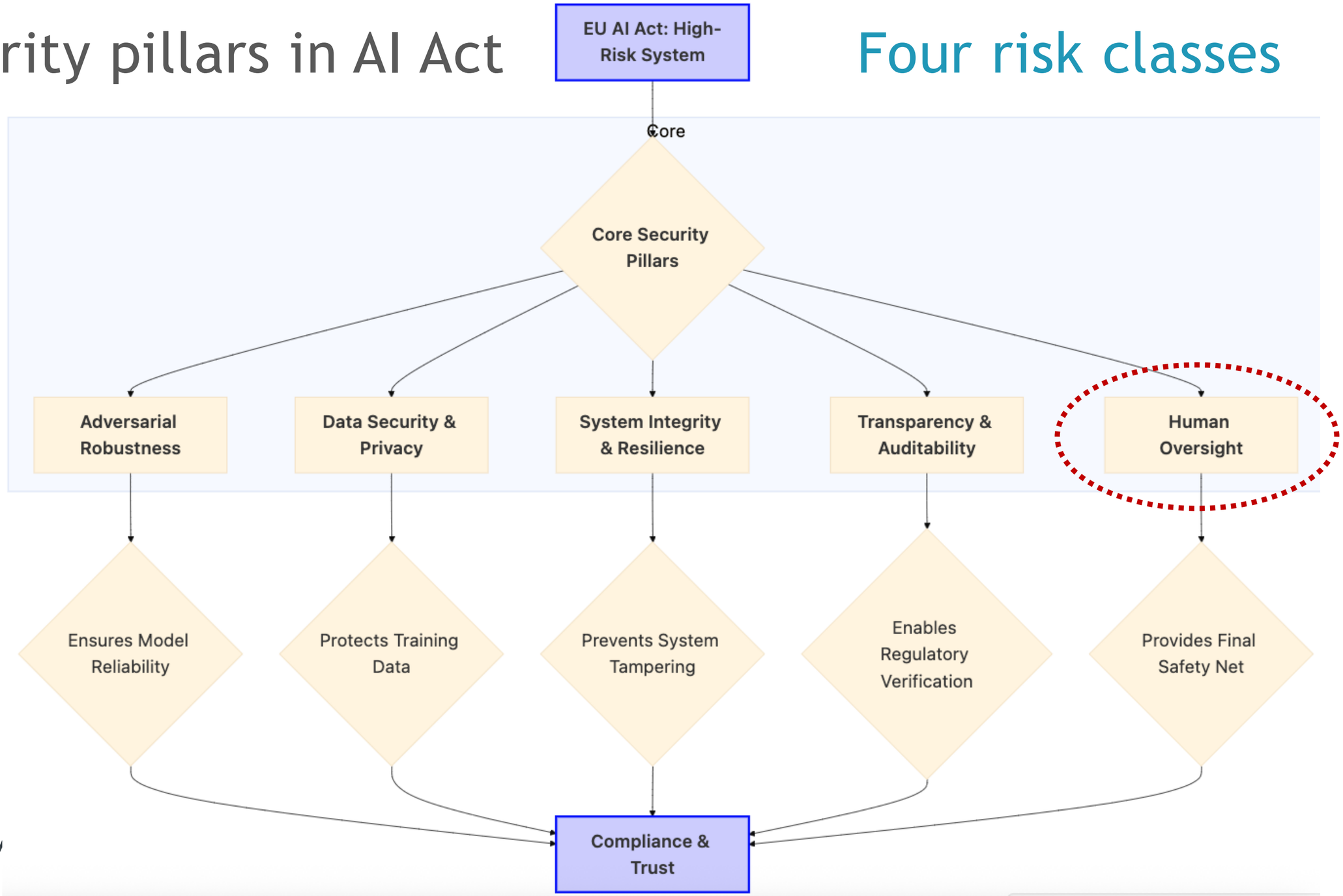
EU directives, e.g.

- GDPR
- NIS2
- Product Liability Directive “new PLD”

AAVISTA

Security pillars in AI Act

Four risk classes

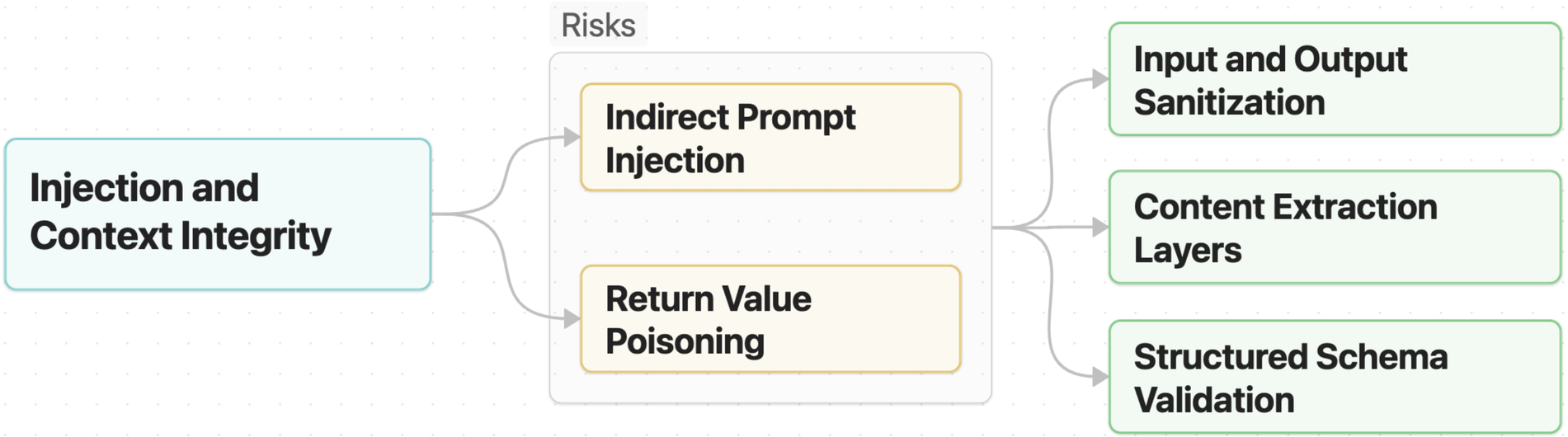


How to secure API access

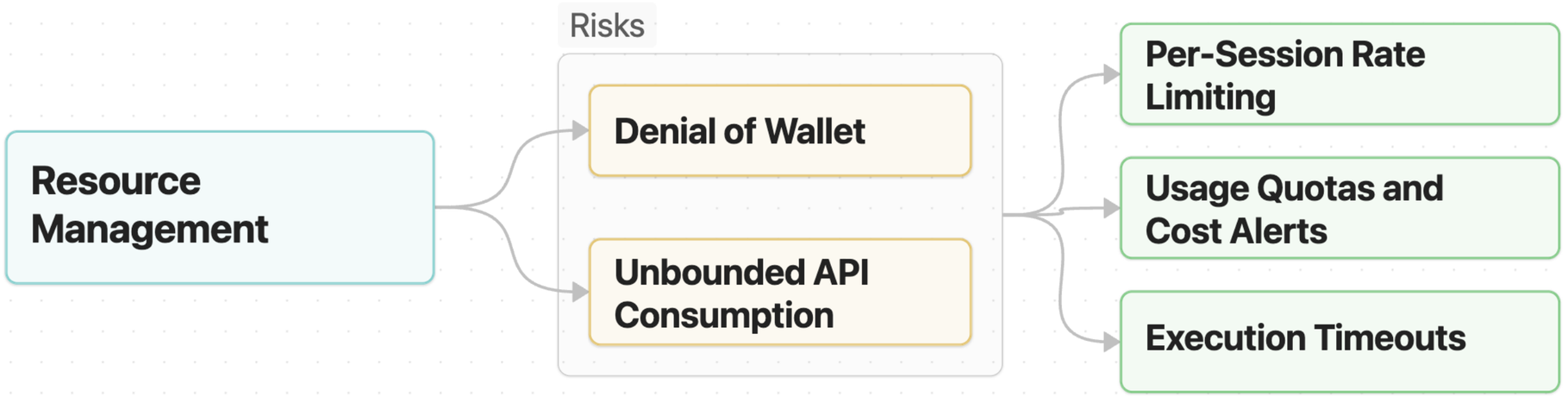
AAVISTA

Access control and authorization

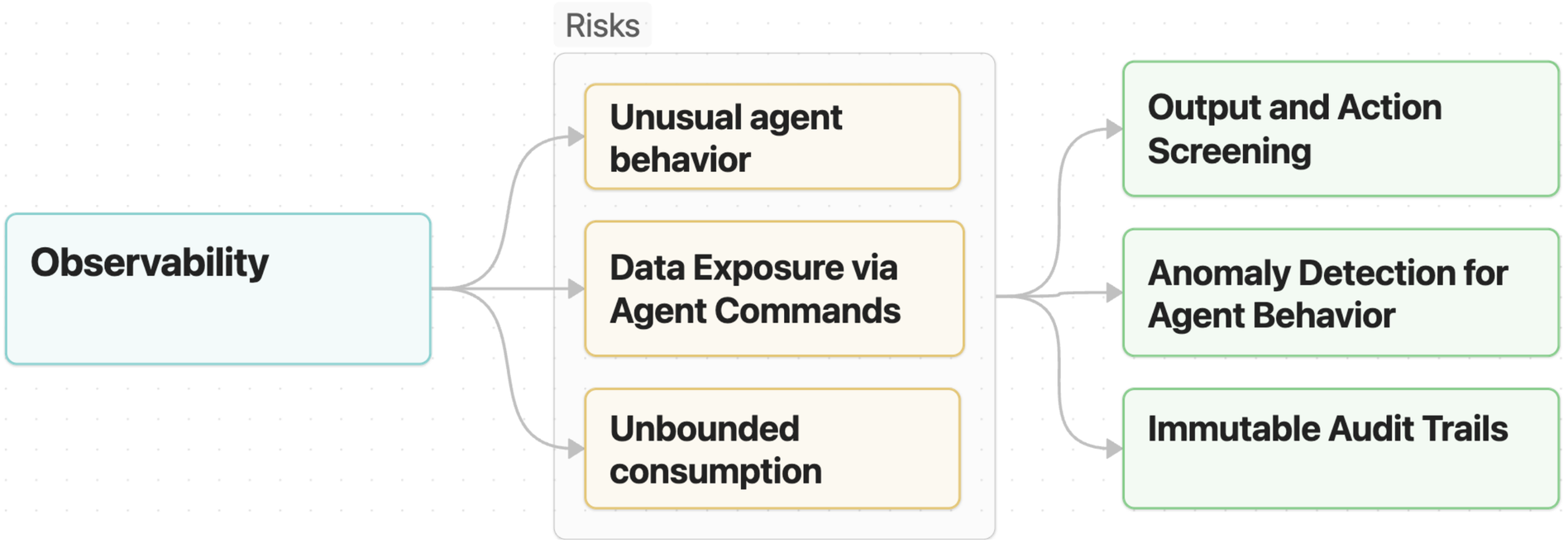
Injection and context integrity



Resource management

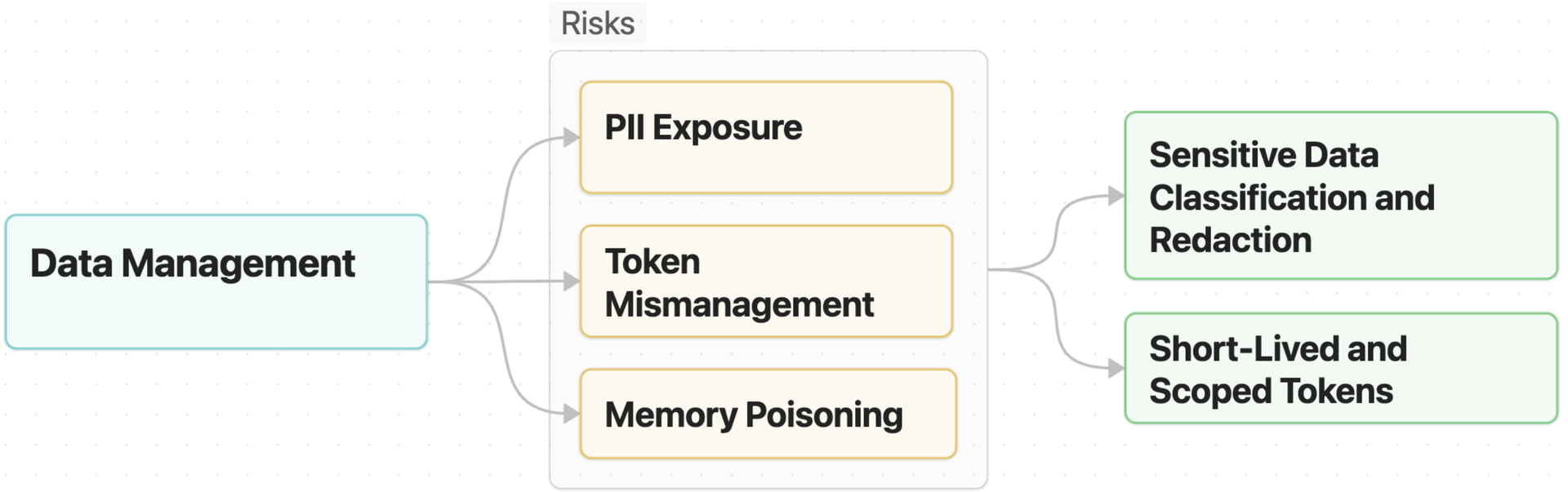


Monitoring and observability



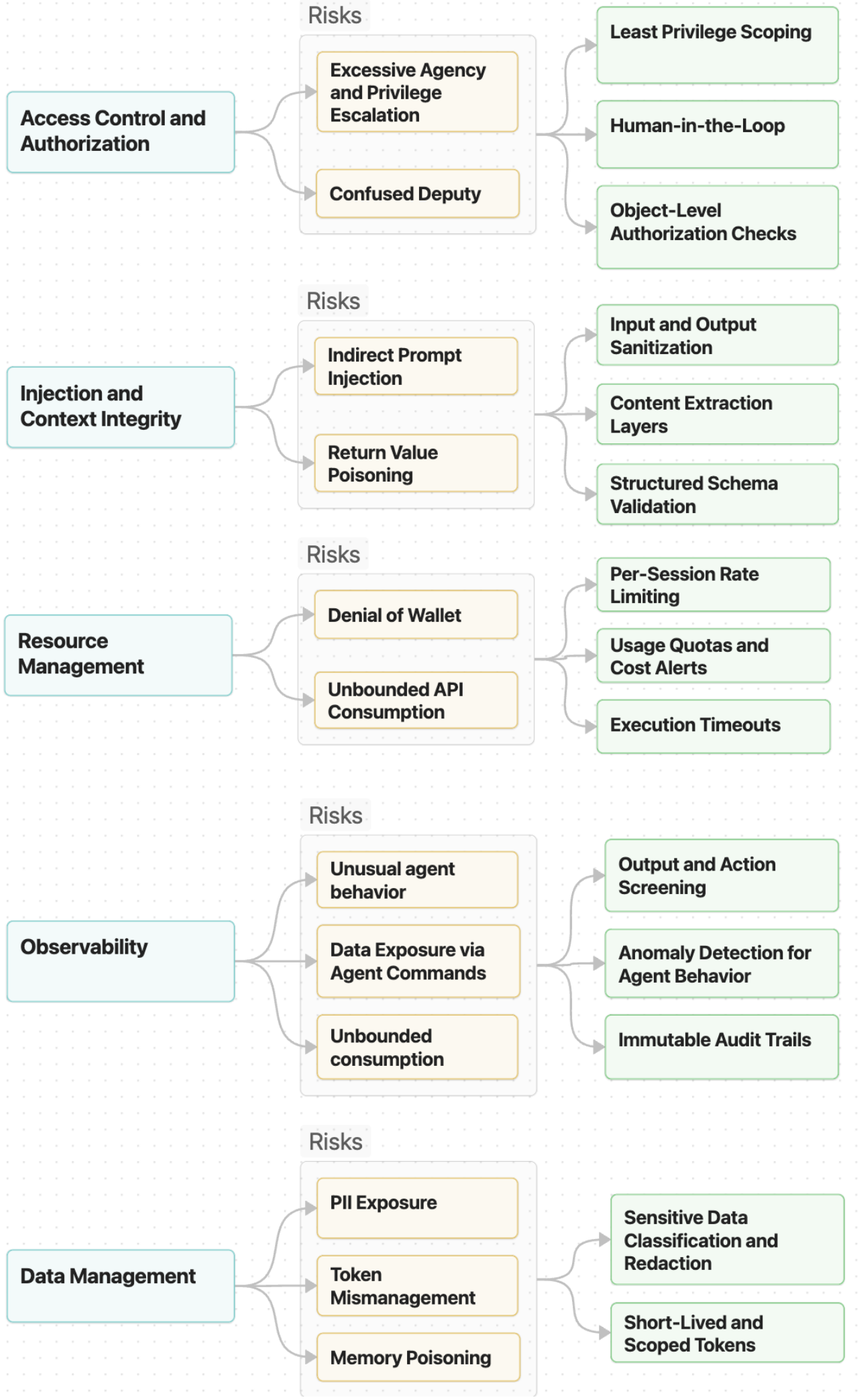
AAVISTA

Data management



AAVISTA

Focus on observability, reaction time, and notifying stakeholders



AAVISTA

Key takeaways

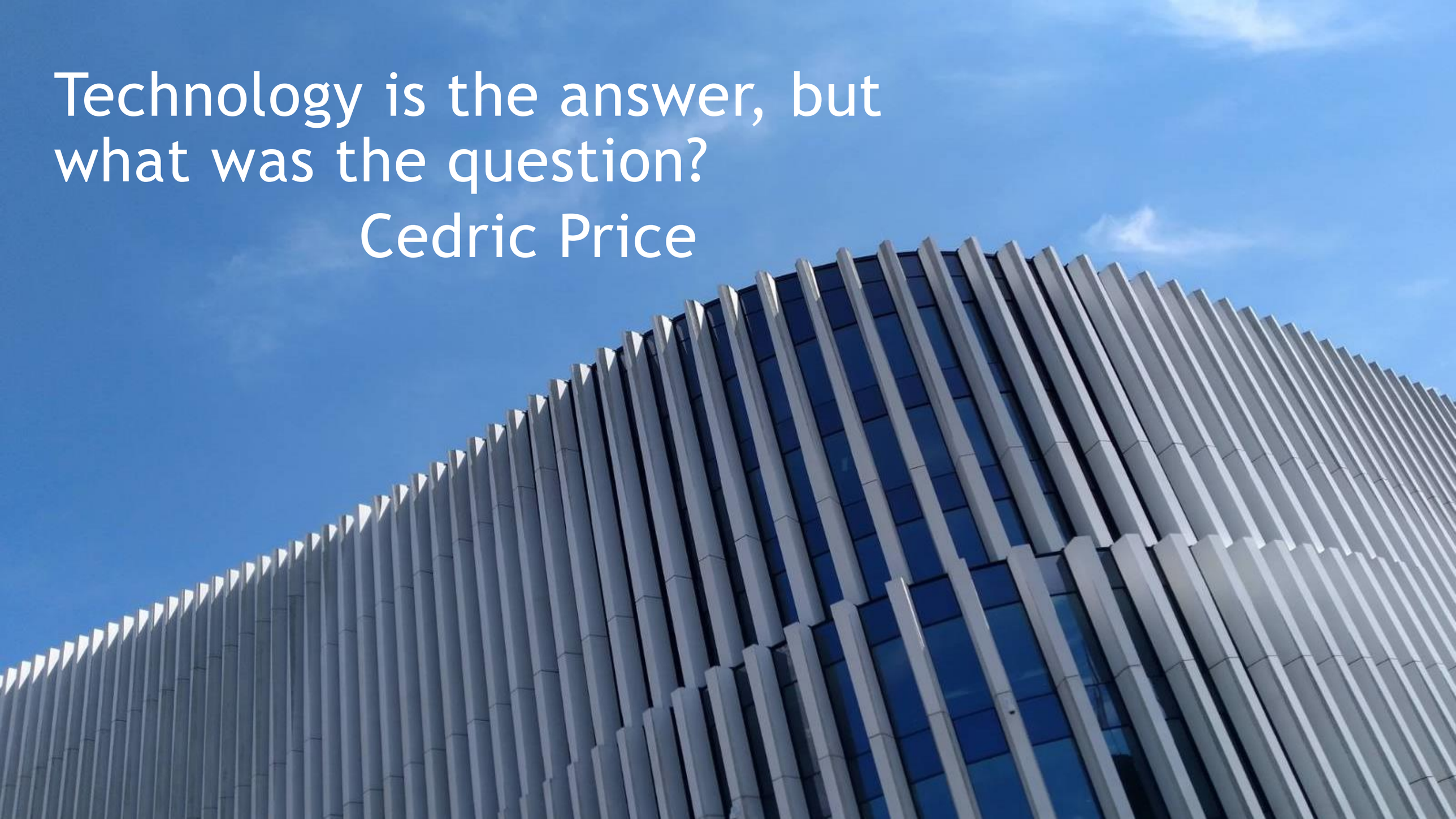
Govern the AI.

Allow only the minimal access.

Design and build observability from the start.

Remember Human-in-the-Loop.

AAVISTA


Technology is the answer, but
what was the question?
Cedric Price

AAVISTA

The Data Refinery Company

Merja Kajava
https://www.linkedin.com/in/merjakajava