THE PHOBOS GROUP

info@phobos.io
https://phobos.io

PHOBOS AIRLOCK

Safe LLM operations in hostile supply chains

Keynote + Q&A

2 Day Hands-On workshop

CONTAIN

Insulate opaque npm, pypl and model-driven repos currently targeted by supply chain attacks

OBSERVE

Surface supply-chain attacks before they attempt to spread through your environment or loot secrets & tokens

MOVE FAST

Keep LLM-assisted engineering velocity while maintaining separation from sensitive systems & data

A practical containment architecture for teams using **Claude Code**, **Codex** or **other TUI tools**, **npm-heavy** and agentic development workflows and pipelines.

Remember:
Phobos has your back!