

REFERENCE NODE R1 - 180-TAGE-FORSCHUNGSPILOT - PARTNER GESUCHT

Sovereign AI Security Node R1

Partner-Brief für lokale souveräne KI, sichere Codeanalyse und Agentic-AI-Assurance

SKOPION plant eine professionelle Workstation-Zielarchitektur für reproduzierbare lokale KI-, Software-Security- und private Cybersecurity-Workloads. Reference Node R1 ist ein kontrollierter 180-Tage-Forschungspilot mit messbaren Gates und menschlicher Validierung.

R1 ist eine Zielarchitektur, kein bereits vorhandenes System. SKOPION behauptet weder den Besitz der genannten Komponenten noch eine Partnerschaft oder Empfehlung durch deren Hersteller. Gleichwertige professionelle Plattformen bleiben möglich.

Warum lokale Infrastruktur

Sensible Code-, Incident- und Evidenzdaten passen nicht immer in externe KI-Dienste. Große lokale Modelle, lange Kontexte, deterministische Security-Tools und agentische Testumgebungen brauchen eine belastbare, isolierbare Plattform. Modellmeinungen ersetzen keine Evidenz.

Reference Node R1 - Zielarchitektur

- CPU - AMD Ryzen Threadripper PRO 9985WX, 64-Core-Klasse, oder gleichwertige professionelle Workstation-Plattform.
- GPU - 1 x NVIDIA RTX PRO 6000 Blackwell, 96 GB ECC VRAM; Max-Q 96 GB als energieeffiziente Alternative.
- RAM - 256 GB DDR5 ECC RDIMM.
- Storage - 2 TB NVMe System plus 8 TB NVMe AI/Daten oder gleichwertig sicher segmentiert.
- Netzwerk - 10 GbE Ziel; kontrollierte Datenpfade, kein unkontrollierter Fernzugriff.
- OS - Ubuntu 24.04 LTS; Windows 11 Pro / WSL2 nur bei begründetem Toolbedarf.

180-Tage-Pilot

- Phase 1 - Baseline & Hardening: Deployment, Isolation, Reproduzierbarkeit.
- Phase 2 - Local AI: LLM/VLM, Kontext, Speicher und Datenlokalität.
- Phase 3 - Software Security: sichere Codeanalyse, Tool-Korrelation und Triage.
- Phase 4 - Agentic AI: autorisierte Tool-Use- und Multi-Agent-Assurance.
- Phase 5 - Optimierung: Performance, Leistung, Thermik und Stabilität.
- Phase 6 - Report: Benchmarks, Architekturfolgerungen und sicherer Demonstrator.

Workloads und messbare Gates

- Local AI: 70B-Klasse soweit Architektur und Quantisierung erlauben; Long Context, Embeddings, Reranking, private RAG.
- Secure Software Analysis und Fuzzing Support: CPU kompiliert/testet, AI unterstützt Clustering, Harness-Analyse und Triage.
- Agentic AI Assurance: Prompt Injection, Excessive Agency, RAG- und Tool-Use-Sicherheit.
- OSINT/EASM/Incident: öffentliche Quellen, Klassifikation und Evidenzstrukturierung.
- LoRA/QLoRA, domänenspezifische Embeddings, Reranker und Klassifikatoren, soweit technisch sinnvoll.
- Messung: Reproduzierbarkeit, Latenz, Durchsatz, Ressourcen, Stabilität, Leistung, Datenlokalität und False Positives.

Technology partnership

- Modelle: Evaluation Workstation, GPU/CPU/Plattform, 180-Tage-Leihstellung, Komponentenbeitrag oder Projektkonditionen.
- SKOPION liefert reproduzierbare Benchmarks sowie Kompatibilitäts-, Stabilitäts- und Architekturfeedback.
- Möglich: sicherer Demonstrator und gemeinsam freigegebene anonymisierte Fallstudie.
- Öffentliche Nennung ausschließlich nach schriftlicher Zustimmung.
- Keine Kundendaten, Zugangsdaten, unveröffentlichten Schwachstellen oder unkontrollierter Remote-Zugriff.

Klare Grenzen

Keine nicht autorisierten oder produktionsstörenden Tests. Keine Zero-Day-, Finding- oder Payout-Versprechen. Keine Förder-, Programm-, Eigentums- oder Partnerschaftsbehauptung ohne veröffentlichte Bestätigung.

Technologiepartnerschaft besprechen: <https://skopion.de/de?topic=research-partnership#contact>