

REFERENCE NODE R1 - 180-DNIOWY PILOTAŻ BADAWCZY - SZUKAMY PARTNERÓW

Sovereign AI Security Node R1

Brief partnerski: lokalne sovereign AI, bezpieczna analiza kodu i agentic-AI assurance

SKOPION planuje docelową architekturę profesjonalnej stacji roboczej do powtarzalnych lokalnych workloadów AI, software security i prywatnego cyberbezpieczeństwa. Reference Node R1 to kontrolowany 180-dniowy pilotaż badawczy z mierzalnymi bramkami i walidacją człowieka.

R1 jest architekturą docelową, a nie posiadanym obecnie systemem. SKOPION nie deklaruje posiadania wymienionych komponentów, partnerstwa z producentami ani ich rekomendacji. Równoważne profesjonalne platformy pozostają w zakresie.

Dlaczego infrastruktura lokalna

Wrażliwy kod, dane incydentów i dowody nie zawsze powinny trafiać do zewnętrznych usług AI. Duże modele lokalne, długi kontekst, narzędzia deterministyczne i agentowe środowiska testowe wymagają stabilnej, izolowalnej platformy. Opinia modelu nie zastępuje dowodu.

Reference Node R1 - architektura docelowa

- CPU - AMD Ryzen Threadripper PRO 9985WX, klasa 64 rdzeni, lub równoważna profesjonalna platforma workstation.
- GPU - 1 x NVIDIA RTX PRO 6000 Blackwell, 96 GB ECC VRAM; Max-Q 96 GB jako wariant energooszczędny.
- RAM - 256 GB DDR5 ECC RDIMM.
- Storage - 2 TB NVMe system plus 8 TB NVMe AI/dane albo równoważny bezpiecznie segmentowany układ.
- Sieć - cel 10 GbE; kontrolowane ścieżki danych i bez niekontrolowanego zdalnego dostępu.
- OS - Ubuntu 24.04 LTS; Windows 11 Pro / WSL2 tylko przy uzasadnionym wymaganiu narzędzia.

180-dniowy pilotaż

- Faza 1 - Baseline & Hardening: wdrożenie, izolacja i powtarzalność.
- Faza 2 - Local AI: inferencja LLM/VLM, kontekst, pamięć i lokalność danych.
- Faza 3 - Software Security: bezpieczna analiza kodu, korelacja i triage.
- Faza 4 - Agentic AI: autoryzowana ocena tool-use i multi-agent.
- Faza 5 - Optymalizacja: wydajność, pobór mocy, termika i stabilność.
- Faza 6 - Raport: benchmarki, wnioski architektoniczne i bezpieczny demonstrator.

Workloady i mierzalne bramki

- Local AI: klasa 70B, gdy pozwala architektura i kwantyzacja; długi kontekst, embeddings, reranking i prywatny RAG.
- Secure Software Analysis i Fuzzing Support: CPU kompiluje/testuje; AI wspiera clustering, harness analysis i triage.
- Agentic AI Assurance: prompt injection, excessive agency, bezpieczeństwo RAG i tool-use.
- OSINT/EASM/Incident: źródła publiczne, klasyfikacja i strukturyzacja dowodów.
- LoRA/QLoRA, domenowe embeddings, rerankery i klasyfikatory, jeśli są technicznie uzasadnione.
- Pomiary: powtarzalność, latencja, przepustowość, zasoby, stabilność, energia, lokalność danych i false positives.

Technology partnership

- Modele: evaluation workstation, GPU/CPU/platforma, użyczenie 180 dni, wkład komponentowy lub warunki projektowe.
- SKOPION może dostarczyć benchmarki oraz feedback o kompatybilności, stabilności i architekturze.
- Opcjonalnie: bezpieczny demonstrator i wspólnie zatwierdzone anonimowe case study.
- Publiczne podziękowanie wyłącznie po pisemnej zgodzie.
- Bez danych klientów, poświadczeń, nieopublikowanych podatności i niekontrolowanego remote access.

Jasne granice

Bez testów nieautoryzowanych lub zakłócających produkcję. Bez obietnic zero-dayów, liczby ustaleń lub payoutów. Bez deklaracji finansowania, programu, posiadania lub partnerstwa bez publicznego potwierdzenia.

Porozmawiaj o partnerstwie technologicznym: <https://skopion.de/pl?topic=research-partnership#contact>