Agentic AI mit Open Source

SwissICT #DIGITUP
5. Mai 2026

Dani Rütimann · Michael «Eichi» Eichenberger · Niklaus «Nik» Hofer

SAMSTAG, 02:00 UHR

48

48

ungelesene Security Advisories

Dani Rütimann

Michael Eichenberger

Niklaus Hofer

Ablauf

- Einführung
  - 15 Minuten
- Workshop
  - 70 Minuten
- Abschluss mit Fazit
  - 10 Minuten

Chatbot versus Agent

Chatbot

- Wartet auf Fragen
- Ein Schritt
- Vergisst

Agent

- Handelt selbständig
- Plant & nutzt Werkzeuge
- Lernt dazu
- Arbeitet rund um die Uhr

Wo unterstützt ein Agent?

stepping stone

Security Monitoring

E-Mail Triage

Reporting

Kunden Updates

Datenaufbereitung

System Updates

Agent: **wenige 100 CHF / Monat**

Mitarbeitende: ~~6'000 bis 10'000 CHF/Monat~~

Hermes Agent

stepping stone

Open Source

Keine Black Box

Vollständig einsehbar, anpassbar, kontrollierbar

Schweizer Infrastruktur

stepping stone AG Cloud

Daten bleiben in der Schweiz

Self-learning

Wird besser über Zeit

Jeder Einsatz trainiert neue Skills

Multi-Modell

Spezialisierte Modelle

Pro Aufgabe das passende Modell

Agentic-Modelle: MiniMax-M2.5 · Nemotron-3-Super-120B · Qwen3-Coder-Next · Qwen/Qwen3.5-35B-A3B-FP8 · ...
Plus Spezialmodelle für OCR, Suche, Sprache

Mehrere Ebenen

stepping stone

SOUL.md

Persönlichkeit

- **Ton & Stil**
- **Identität**
- **Werte & Haltung**

AGENTS.md

Projektwissen

- **Workflows**
- **Konventionen**
- **Kontextwissen**

Tools

Eingebaute Fähigkeiten

- **Neue Fähigkeiten**
- **Eingebaut**
- **Nach Sets organisiert**

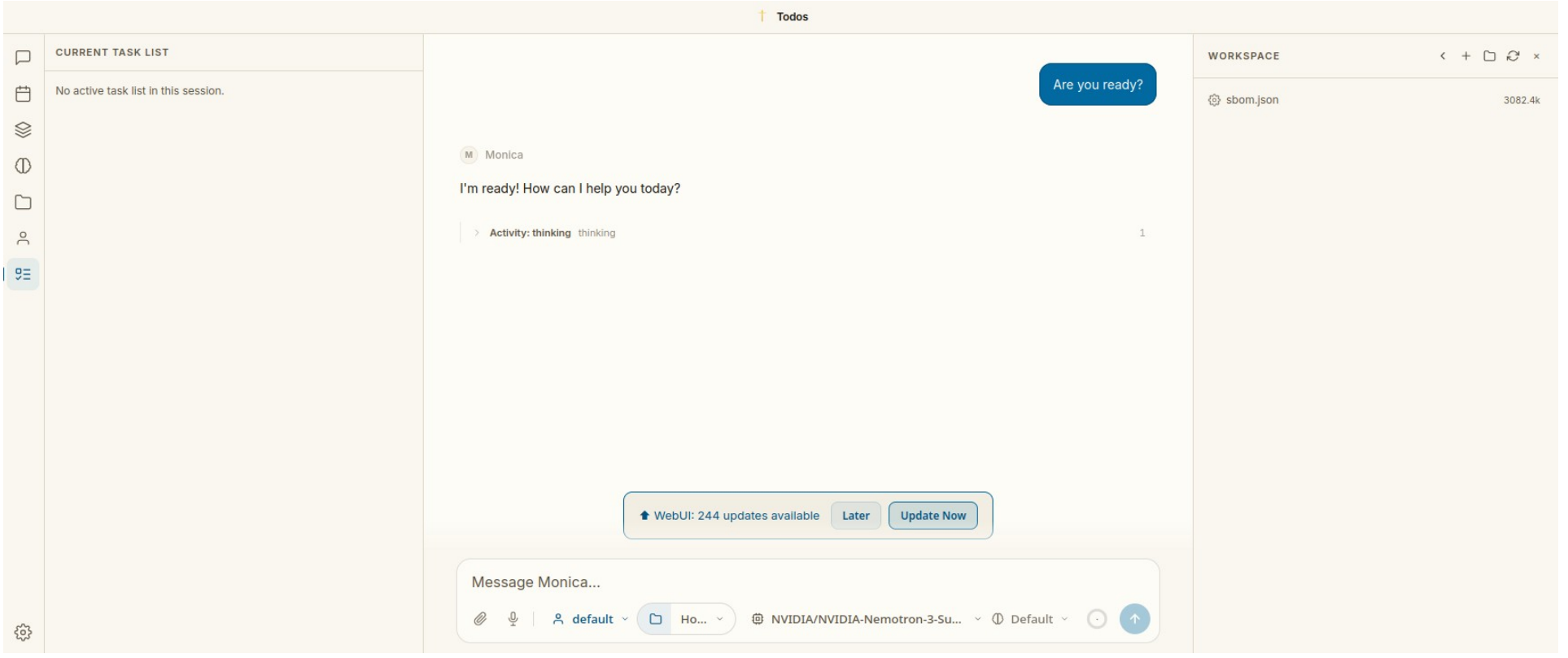
Skills

Erlernte Fähigkeiten

- **On-demand**
- **Gelerntes Wissen**
- **Erweiterbar**

Hermes WebUI

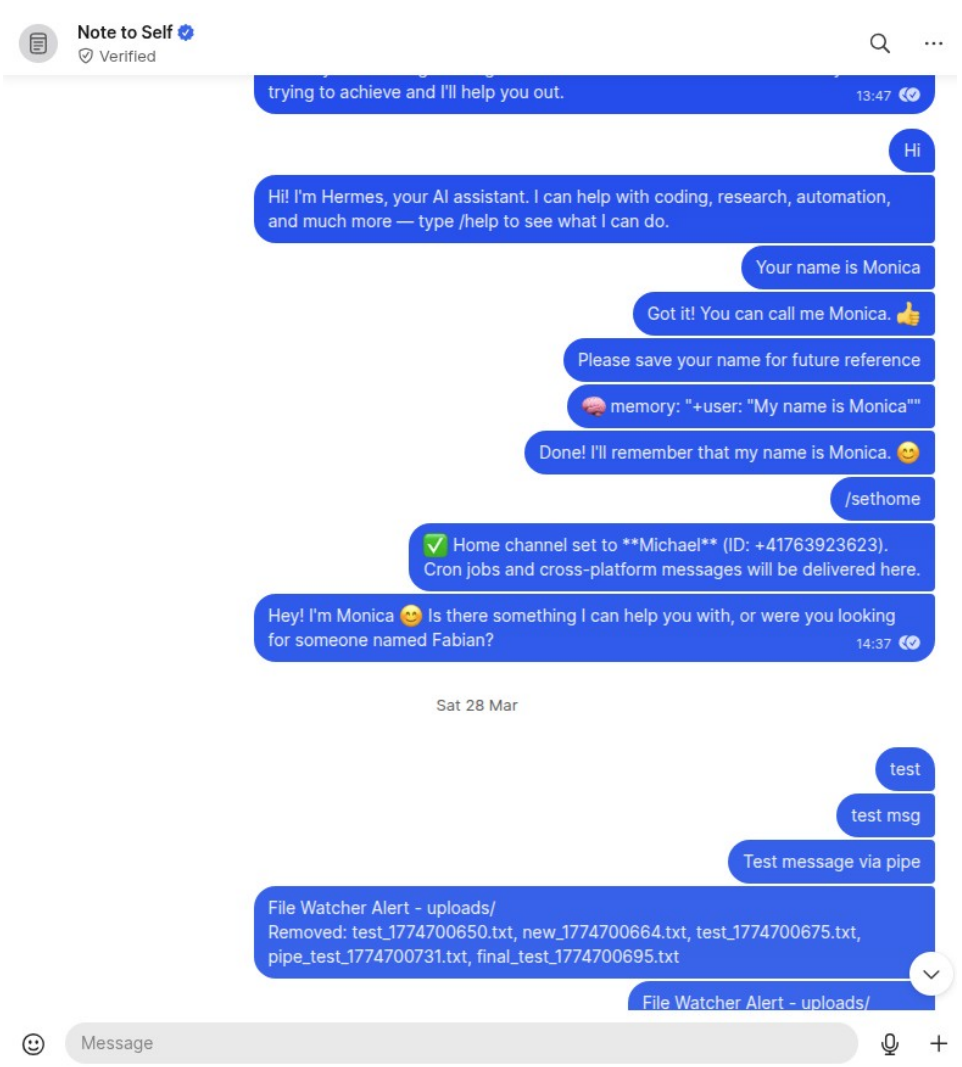
stepping stone



CLI


HERMES-AGENT
Hermes Agent v0.9.0 (2026.4.13) · upstream e69526be · local 588985b0 (+12 carried commits)
NVIDIA-Nemotron-3-Super-1... · Nous Research
/home/sst-mei
Session: 20260503_102713_053838
Available Tools
browser: browser_back, browser_click, ...
clarify: clarify
code_execution: execute_code
cronjob: cronjob
delegation: delegate_task
file: patch, read_file, search_files, write_file
homeassistant: ha_call_service, ha_get_state, ...
image_gen: image_generate
(and 12 more toolsets...)
MCP Servers
swiss (stdio) — 31 tool(s)
Available Skills
autonomous-ai-agents: claude-code, codex, hermes-agent, opencode
creative: architecture-diagram, ascii-art, ascii-video, e...
data-science: jupyter-live-kernel
devops: webhook-subscriptions
email: himalaya
gaming: minecraft-modpack-server, pokemon-player
general: dogfood, hermes-interactive-commands, interacti...
github: codebase-inspection, github-auth, github-code-r...
leisure: find-nearby
mcp: mcporter, native-mcp
media: gif-search, heartmula, songsee, youtube-content
mlops: audiocraft-audio-generation, axolotl, clip, dsp...
note-taking: obsidian
productivity: check-service-usage, google-workspace, investig...
red-teaming: godmode
research: arxiv, blogwatcher, github-repo-evaluation, llm...
smart-home: openhue
social-media: xitter
software-development: code-review, plan, requesting-code-review, safe...
stepping-stone: almalinux-security-mail-monitor, create-project...
59 tools · 101 skills · 1 MCP servers · /help for commands
Welcome to Hermes Agent! Type your message or /help for commands.
Tip: MCP subprocesses receive a filtered environment — only safe system vars pass through.
NVIDIA-Nemotron-3-Super... | ctx -- | [ ] -- | 40s

Signal


Note to Self
Verified
trying to achieve and I'll help you out.
13:47
Hi
Hi! I'm Hermes, your AI assistant. I can help with coding, research, automation, and much more — type /help to see what I can do.
Your name is Monica
Got it! You can call me Monica. 👍
Please save your name for future reference
🧠 memory: "+user: "My name is Monica""
Done! I'll remember that my name is Monica. 😊
/sethome
✅ Home channel set to **Michael** (ID: +41763923623). Cron jobs and cross-platform messages will be delivered here.
Hey! I'm Monica 😊 Is there something I can help you with, or were you looking for someone named Fabian?
14:37
Sat 28 Mar
test
test msg
Test message via pipe
File Watcher Alert - uploads/
Removed: test_1774700650.txt, new_1774700664.txt, test_1774700675.txt, pipe_test_1774700731.txt, final_test_1774700695.txt
File Watcher Alert - uploads/
Message

MCP Server

```
🚆 Transport    – SBB, PostBus, trams, live departures, journey planning
🌤️ Weather      – MeteoSwiss live conditions + historical data
🌊 Hydrology    – BAFU river & lake levels (great for Aare swimming!)
🗺️ Geodata      – swisstopo geocoding, solar potential, geographic layers
🏢 Companies    – ZEFIX federal registry, all 700K+ Swiss companies
🎄 Holidays     – Swiss public & school holidays by canton
🏛️ Parliament   – Bills, votes, members, speeches, cantonal affairs (OpenParlData.ch)
🏔️ Avalanche    – SLF danger bulletins and warning regions
💨 Air Quality  – NABEL stations, Swiss legal limits (LRV)
📮 Swiss Post   – Postcode lookup and parcel tracking
⚡ Energy       – Electricity tariffs by municipality (ElCom)
📊 Statistics   – Population, demographics, BFS datasets
🏦 SNB Rates    – Swiss National Bank CHF exchange rates, historical data
♻️ Recycling    – Zurich city waste collection calendar (OpenERZ)
📰 Swiss News   – SRF news headlines and keyword search
🗳️ Voting       – Swiss popular vote results (Basel-Stadt open data)
🌊 Dams         – Swiss federal dam registry (SFOE/swisstopo)
🥾 Hiking       – Swiss trail closures and hiking alerts (swisstopo)
🏠 Real Estate  – Swiss property prices, rent index, housing data (BFS)
🚗 Traffic      – ASTRA counting stations, daily volumes
🌍 Earthquakes  – Swiss Seismological Service (SED/ETH Zürich), FDSN API
```

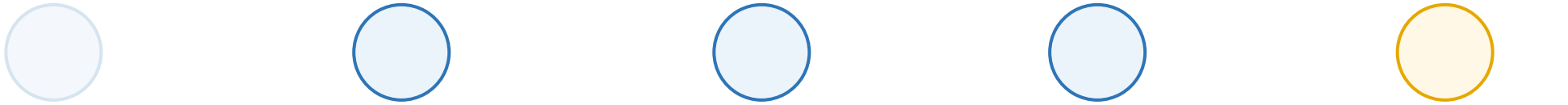
Information Security Management System nach ISO 27001

stepping stone

Security Advisories

- **Enhancement**: No reaction.
- **Bug fix**: Implement in the monthly maintenance window.
- **Low impact**: Implement in the monthly maintenance window.
- **Moderate impac**t: Implement in the monthly maintenance window.
- **Important impact**: A judgement call has to be made here.
- **Critical impact**: Apply as soon as possible.

Workflow



E-Mail

Hermes wertet Security Advisory

Hermes gleicht Software mit SBOM ab

Hermes arbeitet die Software Errata ab

Hermes installiert Pakete auf dem Mirror

100 – 150

Stunden / Jahr

zurückgewonnen

24 / 7

Verfügbarkeit

gleiche Qualität, egal wann

Workshop

Jetzt seid ihr dran

In Zweierteams: Euer Hermes wartet.

Security Advisories liegen bereit.

Security Advisory Analyse

Szenario: Du bist CISO. Deine Mailbox hat Security Advisories – und es kommen laufend neue dazu. Hermes ist dein Sicherheitsassistent.

- «Schau dir die Mails an – welche Security-Announcement-Schweregrade sind vorhanden? Zeig mir eine Übersicht.»
- «Prüfe, ob die betroffene Software in meiner SBOM vorkommt.»
- «Gib mir eine priorisierte Liste: Was muss ich sofort tun, was kann warten?»
- «Filtere die Moderate-Meldungen raus – konzentriere dich nur auf **Important** und **Critical**.»

Freie Exploration

Swiss Open Data (mcp-swiss): Firmeninfos über Zefix, Hydrologie-Daten, Aare-Temperatur

- «Wie heisst der VRP von der Stadler Rail AG (via MCP Swiss)?»
- «Wann fährt der nächste Zug nach Bern?»
- «Wie warm ist die Aare in Bern?»

Eigene Fragen

- «Was würdest du in meinem Unternehmen automatisieren?»

Was habt ihr erlebt?

- Was hat überrascht?
- Wo waren die Grenzen?
- Einsatzszenarien in eurem Unternehmen?

Ein Skill. Beliebig erweiterbar.

«Hermes wird nicht neu gestartet – er wächst mit.»

Was kommt als Nächstes?

Threema-Integration

Gesponsert von stepping stone AG

Swiss-Messenger als weiterer Kanal

Hermes as a Service

Security-Bot als Dienstleistung

Für KMU ohne eigene Infrastruktur

Neue Anwendungsfelder

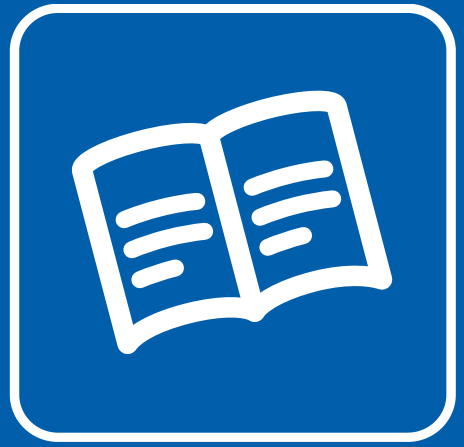
Laufend in Entwicklung

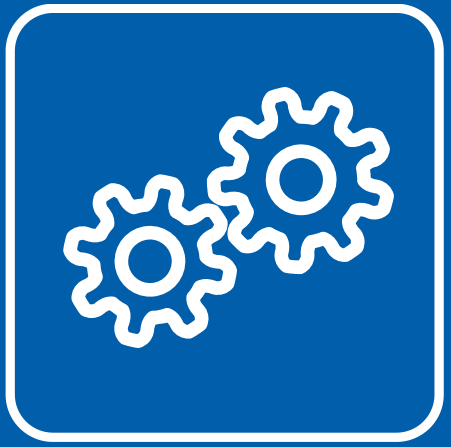
z.B. Unterstützung für betagte Menschen

Fragen?









Save the Date

Nächste Anlässe

- Uphill Conf: Freitag, den 8. Mai 2026
- Sommer Raclette: Donnerstag, den 18. Juni 2026
- Schichtwechsel: Freitag, den 4. September 2026
- B2B Töggälä: Mittwoch, den 21. Oktober 2026
- DINAcon: Mittwoch, den 18. November 2026
- Glühweinapéro: Freitag, den 18. Dezember 2026

Der Agent ist wach.

dani-knows-ai
Wasserwerkgasse 31
3011 Bern

Telefon: +41 79 341 32 51
www.dani-knows-ai.com
hello@dani-knows-ai.com

stepping stone AG
Wasserwerkgasse 7
3011 Bern

Telefon: +41 31 332 53 63
www.stepping-stone.ch
info@stepping-stone.ch