Elias Leslie — Security Automation Summary

Last updated: 2026-06-07

Positioning

Elias Leslie builds AI-assisted security automation and infrastructure tooling with emphasis on secure defaults, repeatable installs, auditable checks, clean release paths, and practical operator workflows.

Public proof points

The repositories below are public and presented by theme rather than ranked.

SummitFlow: Public task orchestration and evidence-capture control plane for AI-assisted development, with a FastAPI backend, Next.js operator UI, Hatchet workflows, the st CLI, and runtime smoke-evidence capture. Release work included secret/history scanning, dependency remediation, Apache-2.0 licensing, CI, local runtime smoke checks, and clean install verification. Repository: https://github.com/elias-leslie/summitflow

Agent Hub: Public self-hosted control plane for multi-provider AI agents, sessions, credentials, prompts, memory, routing telemetry, and a Python SDK. Pairs with SummitFlow as its routed-agent backend and runs standalone. Repository: https://github.com/elias-leslie/agent-hub

Security Hardening Automation (SHA): Public clean-room hardening automation platform for Windows and Linux endpoints with a FastAPI control plane, Next.js operator dashboard, approval-boundary model, generated schemas, public-source starter controls, and clean Proxmox install verification. Repository: https://github.com/elias-leslie/sha

Aico: Public Linux desktop companion for terminal AI agents. Release work included secret/history scanning, standalone docs, Apache-2.0 licensing, CI, local runtime smoke checks, and clean Proxmox install verification. Repository: https://github.com/elias-leslie/aico

A-Term: Public browser workspace for AI coding agents, shells, files, prompts, and notes. Repository: https://github.com/elias-leslie/a-term

Portfolio AI: Public full-stack investment intelligence workspace. Portfolio materials do not show real balances, holdings, transactions, account IDs, brokerage names tied to real data, or live portfolio values. Repository: https://github.com/elias-leslie/portfolio-ai

Portfolio: Public Markdown/PDF proof hub for released projects, with safe visual assets and current links. Repository: https://github.com/elias-leslie/portfolio

Skills demonstrated

- Security automation design: hardening posture, source provenance, approvals, evidence, rollout and rollback thinking.
- Agentic AI tooling: terminal agents, browser context capture, prompt/session infrastructure, multi-provider routing, supervised automation boundaries.

- Full-stack systems: FastAPI, Next.js/Electron, PostgreSQL/Redis-style service design, workflow orchestration, Linux runtime integration.
- Public release discipline: license, docs, config examples, secret scanning, dependency remediation, CI, smoke testing, clean install verification.

Contact

LinkedIn: https://linkedin.com/in/elias-leslie

GitHub: https://github.com/elias-leslie