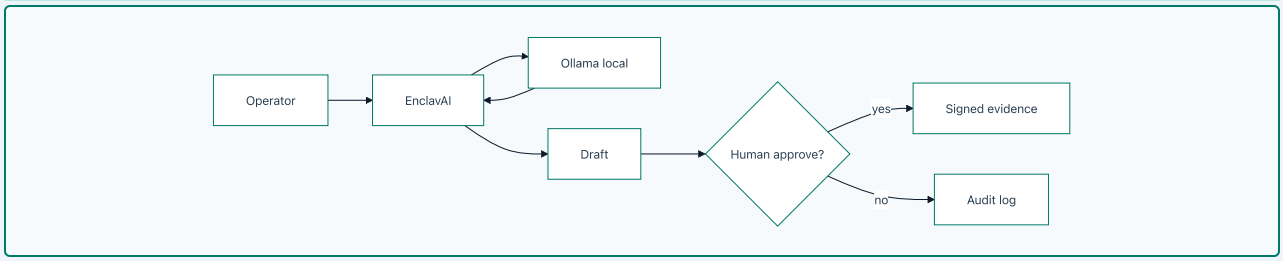
EnclavAI Security Sketch

Self-hosted AI for STIG, POA&M, and SSP work — inside your authorization boundary.

This is a reviewer-facing summary for ISSOs, security architects, and assessors evaluating in-boundary AI. **It is not CMMC certification, a System Security Plan, or legal advice.** Your SSP and ATO package describe the instance you operate.

Architecture (your enclave)



Deploy with Docker Compose on-prem, Azure Gov, AWS GovCloud, or air-gapped. **No cloud LLM API calls during inference.** Optional network-layer egress lock (iptables OUTPUT DROP, IPv4+IPv6).

Security controls

CONTROL	DESIGN
Zero egress	App-layer URL allowlist before any socket opens; optional iptables lock in container
Local inference	Ollama on-host or containerized — open-weight models you approve
Human gate	Generated scripts stay `draft` until an approver approves or rejects
Safety scan	Deterministic destructive-command backstop (bash, PowerShell, Ansible)
Evidence	Tamper-evident HMAC-signed packages; offline verify without EnclavAI
Identity	RBAC (admin / analyst / read-only); HMAC-signed bearer tokens; audited actions

Does / does not

ENCLAVAI DOES	ENCLAVAI DOES NOT
Ingest STIG/XCCDF, `.ckl`, SCAP, Nessus	Certify your organization for CMMC
Draft remediation, POA&M, SSP sections locally	Replace your ISSO or C3PAO
Log user, model, prompt, disposition	Auto-execute remediation on production systems
Export per-artifact evidence for assessors	Send CUI to commercial AI SaaS

Public site vs product: the free STIG scorer runs in your browser only — do not submit CUI there. The self-hosted product is designed under *your* CUI program inside *your* boundary.

Product: enclavai.io · **Free STIG scorer (browser-only):** enclavai.io/tools/stig-scorer/ · **Design partners:** enclavai.io/#pilot · **Full security page:** enclavai.io/legal/security

Gnukum Cloud Solutions · Darelim & GnukuM LLC · June 2026