Sammā Suit *MEGA CHEATSHEET*

SECURITY GOVERNANCE FRAMEWORK FOR AI AGENTS

ONEZEROEIGHT.AI
2026 Edition

ENFORCEMENT ORDER — EVERY API CALL

① SUTRA → ② DHARMA → ③ SANGHA → ④ KARMA → ⑤ BODHI → ⑥ METTA → ⑦ SILA → ⑧ NIRVANA

🔒 8 SECURITY LAYERS

1	**SUTRA**	Gateway — origin validation, rate limit, TLS
2	**DHARMA**	Permissions — 33 perms, 7 roles, RBAC
3	**SANGHA**	Skill vetting — allowlist + AST scanning
4	**KARMA**	Cost control — user-set budget ceiling (BYOK)
5	**BODHI**	Isolation — subprocess sandbox, egress allowlist
6	**METTA**	Identity — Ed25519 signing per agent
7	**SILA**	Audit — every call logged with cost tracking
8	**NIRVANA**	Recovery — kill switch, snapshots, rollback

OPENCLAW HOOK MAPPING

NIRVANA	before_agent_start	p:1000
DHARMA	before_tool_call	p:900
SANGHA	before_tool_call	p:800
KARMA	before_agent_start	p:700
BODHI	before_agent_start	p:600
METTA	message_sending	p:500
SILA	after_tool_call	p:100

⚡ API REFERENCE

AGENTS

POST /api/agents	Create agent
GET /api/agents	List all
GET /api/agents/{id}	Detail
PUT /api/agents/{id}	Update
POST /api/agents/{id}/gateway	Chat (all 8 layers)

NIRVANA — KILL & RECOVERY

POST /api/agents/{id}/kill	Kill switch
POST /api/agents/{id}/revive	Revive
GET /api/agents/{id}/snapshots	Snapshot history
POST /api/agents/{id}/rollback/{s}	Restore snapshot

SANGHA — SKILLS & MARKETPLACE

GET /api/marketplace/skills	Browse skills
POST /api/marketplace/skills/import	Upload SKILL.md
POST .../import-clawhub	Import from ClawHub

SILA — AUDIT

GET /api/audit	Full audit log
GET /api/audit?agent_id={id}	Per-agent log

AUTH & BILLING

POST /api/auth/magic-link	Send login email
POST /api/billing/portal	Stripe portal
GET /api/dashboard/health	Health check

🚀 QUICK INSTALL

```
# Standalone
pip install samma-suit

# OpenClaw plugin
openclaw plugins install samma-suit

# Verify
openclaw plugins doctor ✓
```

PLUGIN CONFIG

~/.openclaw/openclaw.json

```
{
  "plugins": {
    "entries": {
      "samma-suit": {
        "enabled": true,
        "config": {
          "api_url":
"https://api.sammasuit.com",
          "api_key": "samma_...",
          "llm_key": "sk-ant-...",
          "budget": 100,
          "layers": ["ALL"]
        }
      }
    }
  }
}
```

PRICING — BYOK (BRING YOUR OWN KEY)

Free	1 agent, 100 calls/mo
Pro $29/mo	5 agents, custom budget ceiling
Team $99/mo	25 agents, custom budget ceiling

You provide your LLM API key. We enforce governance.
KARMA budget ceiling protects *your* spend.

🎯 THREAT MODEL

● CVE-2026-25253 — WebSocket RCE	→ SUTRA
● ClawHavoc — 341 malicious skills	→ SANGHA
● capability-evolver — data exfil to Feishu	→ BODHI
● Runaway cron — $750/mo heartbeat costs	→ KARMA
● Unauthorized tool execution	→ DHARMA
● Agent impersonation / spoofing	→ METTA
● No forensics / compliance gap	→ SILA
● Rogue agent — no off switch	→ NIRVANA

SANGHA SCAN DETECTS

```
os.system() shell injection
subprocess.* process spawn
eval() / exec() code injection
fetch() / requests.* network exfil
open(.env) secret access
__import__ dynamic import
```

📊 DASHBOARD

sammasuit.com/dashboard.html

TABS

Agents	Cards, status, budget gauge, chat
Skills	Browse, import, SANGHA status
Audit	Filter, export CSV/JSON
Live	Real-time activity feed
Costs	Spend tracking, projections
Billing	Plan, invoices, portal

KEYBOARD SHORTCUTS

?	Show help
N	New agent
C	Open chat
K	Kill agent
R	Revive agent
A	Audit tab
S	Skills tab
L	Live feed
$	Costs tab
/	Focus search
Esc	Close modal

FEATURES

- SSE streaming chat
- Hold-to-kill ceremony
- Snapshot timeline + diff
- Exec approval dialogs
- Dark/light theme toggle
- Mobile optimized (iPhone)

🏗️ ARCHITECTURE

STACK

Backend	FastAPI + Python 3.11
Database	PostgreSQL 16
Auth	Magic link (Resend)
Payments	Stripe
Crypto	Ed25519 (METTA)
LLM	Anthropic API
Frontend	Vanilla JS, single file
Deploy	Railway + GitHub Pages

ESSENTIAL PATHS

```
# Production
API         api.sammasuit.com
Dashboard   sammasuit.com/dashboard.html
Docs       sammasuit.com/getting-started.html

# Registry
ClawHub    clawhub.ai/OneZeroEight-ai/samma-suit
GitHub     github.com/OneZeroEight-ai/samma-suit

# Company
Parent     onezeroeight.ai
Discord    discord.gg/4A6ExTnKnK
```

STATS

Tests	163 PASSING
Endpoints	24+
Layers	8/8 ENFORCED
License	MIT