Cyber Defender: Installation Intelligence & Healing Architecture

1. Mission

Use the installation moment -- when the system is still healthy -- to verify, profile, and prepare for future healing. Cyber Defender is designed to protect and restore systems proactively, with AI-powered healing capabilities.

2. Pre-Installation Phase

- Health Check: Runs cyber-healthcheck to validate memory, disk, suspicious processes.

- Decision: Installation proceeds only if the system passes all diagnostics.

3. Installation Phase: Deploying Smart Local AI

- Fingerprint the System: Capture OS, version, model, running services.

- Deploy Local AI: Install local_ai.py to monitor entropy and phase logs.

- Store Emergency Healing Kit: Install system-specific healing scripts.

4. Three-Version Script Lifecycle

Scripts are versioned to evolve safely:

- v1: Basic implementation

- v2: 10-15% improved logic

- v3: Hardened with better fallback

Each version undergoes QA before being compressed and archived.

5. Quality Control Workflow

- Developers write 3 versions

- QA team approves after tests

- Approved scripts are compressed, signed, and stored in modules_verified

6. Healing in Action (Example: MacBook)

If a MacBook (macOS 13.6) fails:

1. Local AI detects error

2. Matches fingerprinted profile

3. Runs matched healing module (e.g., fs_repair.sh)

4. Logs action, optionally consults HQ

7. Outcome

- Predictable

- Transparent

- Self-improving

- QA-controlled

- Works offline or with HQ assistance

8. Next Steps

- Generate CLI tools documentation

- Create customer-facing whitepaper

- Define internal QA checklist templates