

How to Train Your Agent

Deterministic Tool Boundaries, SKILL.md Architecture & Operational Parity

Franklin Diaz

Bitsmasher Lab

October 12, 2026

Disclosure & Independence

- ▶ **Operational Context:** Research, lab designs, and systems automation documented herein reflect personal engineering practices at Bitsmasher Lab.
- ▶ **Vendor Independence:** Technical references to vendor platforms or tools are illustrative and do not constitute an official corporate endorsement.
- ▶ **License & Distribution:** Distributed under the lab's open research terms for technical educational purposes.

Architecture of an Agent Skill

- ▶ **Deterministic Scoping:** SKILL.md defines capabilities, schemas, and operational constraints.
- ▶ **Frontmatter Metadata:** Declarative triggers, dependency matrices, and tool profiles.
- ▶ **Boundary Enforcement:** Strict separation between `group:fs` (read/write workspace) and `group:runtime` (execution/transport).

Operational Guardrails & Parity

- ▶ **Read-Only Auditing:** Auditing ground truth on disk before drafting changes.
- ▶ **Deterministic Handshake:** Machine-verifiable contract states (CONTENT_READY → DEPLOY_COMPLETE).
- ▶ **Parity Verification:** DOM cards == JSON Feed items == physical disk artifacts.