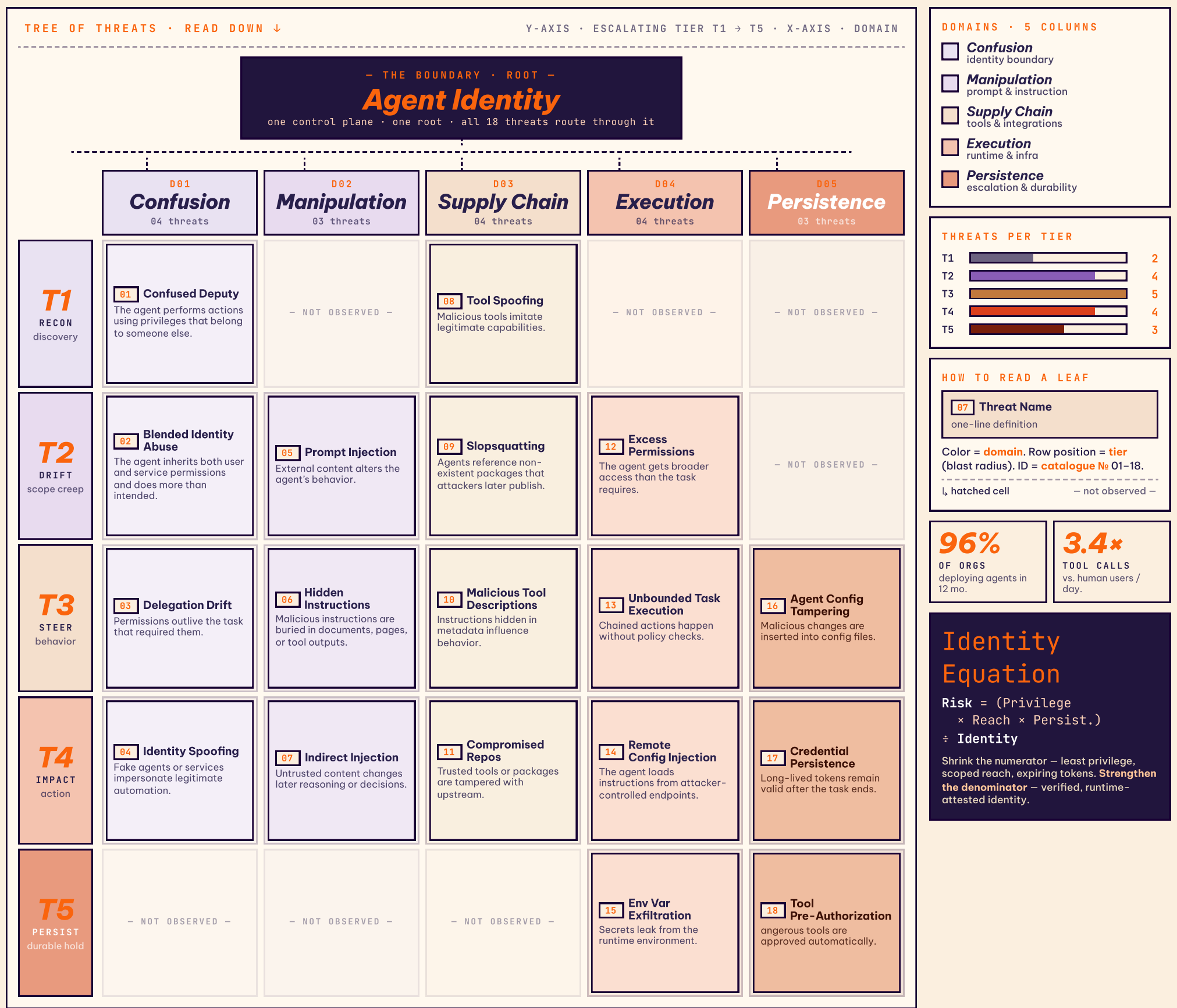


TAXONOMY · 1 BOUNDARY · 5 DOMAINS · 5 TIERS · 18 THREATS

The *Taxonomy* of Agent Threats.

Every threat that AI agents face – classified into a single tree. **One boundary** branches into **five domains**; each domain into **tiers** of escalating blast radius; each tier into named **threats**. Read down to see how a misstep in reasoning becomes catastrophic action.

1 BOUNDARY Identity = the control plane.	5 DOMAINS Reasoning → action.	5 TIERS Escalating blast radius.	18 THREATS All exploit identity gaps.
---	--	---	--



● ENFORCEMENT LAYER

Identity is the *boundary*.

One **vantage point** governs every reasoning step, tool call, and runtime action across all 5 domains.

✓

Delegated identity
Each agent scoped to a user or service.

✓

Short-lived tokens
Credentials expire with the task.

✓

Runtime authorization
Policy at moment of action.

✓

Tool-level policy
Every call passes the same gate.

✓

Immutable audit
Actions tied to specific identity.

✓

Continuous attestation
Identity re-verified per action.

Give every agent an **identity** – and make it the boundary.
See how Aembit applies identity-first controls to AI agents, workloads, and the tools between them.