Tracecat: Free, Open-Source Security Automation That AI Agents Build and Run

Kabui, Charles

2026-07-03

Read at ToKnow.ai

Tracecat is an open-source SOAR platform, short for security orchestration, automation, and response, the software teams use to automate how they respond to security alerts. The difference is that it is built for AI agents. Rather than dragging boxes around a canvas, an engineer describes a job in plain English, such as “triage this phishing report” or “revoke these risky OAuth grants,” and an agent running in Claude Code, Codex, or Copilot builds the workflow

through Tracecat's MCP server. It ships with more than 100 pre-built connectors to security products like CrowdStrike Falcon, Wiz, and Okta, runs long jobs on the durable engine Temporal, and executes untrusted code inside a sandbox using Google's nsjail. It is AGPL-3.0 licensed and self-hostable with Docker or Kubernetes.

Commercial security automation tools are expensive, enterprise-only contracts. Tracecat makes those same SOAR workflows free and self-hosted, so a small team that cannot afford a six-figure platform, or send its alert data to a vendor, can still automate response. Companies like Wealthsimple, SANS, and Depop use it to replace legacy SOAR, and a Depop engineer says they now build agentic workflows they never had time to write by hand.

An agent that can isolate machines and revoke logins is itself a risk, and Tracecat's paid tier leans in: it monitors every agent tool call, lets rules block malicious ones, and requires human approval for sensitive actions. It is the treat your agent as an insider threat idea turned into a product.

Read More: Tracecat's bundled skills are executable add-ons, the kind SkillSpector was built to scan.

Sources:

- Tracecat on GitHub: source, README, and AGPL-3.0 license
- Tracecat docs: the AI-native security automation platform
- Tracecat's open-source SOAR page
- Tracecat's built-in agent skills directory
- nsjail, the Google sandbox Tracecat uses to isolate code
