Project configuration that runs code

Flags repositories whose configuration executes code when an AI agent opens them — a `core.fsmonitor` in `.git/config`, a hook or a `PATH` override in the project's `.claude/settings.json`, an MCP server that starts from `.mcp.json`, a VS Code task that runs on folder open. **Reported, not blocked.**

Why this matters

In 2026 several coding-agent escapes worked the same way: the agent, or a file an attacker got into the repository, wrote configuration that a trusted tool — git, the editor, the agent itself — then ran. Opening the project was enough.

What Sentilai does, and what it does not

The Endpoint Suite checks the projects your developers' agents have opened, on its regular cycle. That means a finding appears **after** the project was opened, not before: this is detection, not prevention. What you get is a record of which repositories carry this kind of configuration and exactly which setting it was — before anyone can clean it up — and the Gateway still governs whatever that code then tries to send.

What is read

Only these files in each project: `.git/config` and the names of executable git hooks, `.claude/settings.json` and `settings.local.json`, `.mcp.json`, `.cursor/mcp.json`, `.codex/config.toml` and `.vscode/tasks.json`. Never your source code, never file contents beyond the setting itself, never environment values — an `env.PATH` override is reported as "env.PATH set", not by its value.

Where you see it

On the device in **Diagnostics**, with the setting and the file it came from. Warning and critical findings also become events in your SIEM export (`project_trust.detected`, and `project_trust.resolved` when a later check no longer finds the setting).

Revision #1
Created 2026-09-29 14:39:35 UTC by Sentilai Docs
Updated 2026-09-29 14:39:35 UTC by Sentilai Docs