What we send to your SIEM

The full list of events Sentilai produces, what each one means, and which fields carry it.

Everything below arrives through **both** delivery modes — the OCSF pull API and the CEF/syslog push. They are the same stream in two formats, not two different feeds.

AI request events

One event per AI request your developers make through the Gateway.

Event	Meaning
`llm_request`	a proxied AI request to any provider
`mcp_call`	an MCP tool call
`mcp_observation`	an MCP tool definition changed on a device
`siem_push_test`	the synthetic event behind **Send test event**

A request that triggered a detector, or that policy blocked, arrives as an **OCSF Detection Finding (class 2004)** — the class your SIEM already routes to an analyst. Everything else is **API Activity (6003)**, the routine "this happened" record.

Each carries: who (user, device), what tool and model, which provider, token counts, duration, outcome, and — when something fired — every detector, every specific finding, and **why it was blocked**.

Ungoverned AI agent events

Autonomous AI agents installed on developer machines that do **not** route through Sentilai.

Event	Meaning
`ungoverned_agent.detected`	an ungoverned agent appeared on a device
`ungoverned_agent.resolved`	it is gone — the developer removed it
`ungoverned_agent.access_blocked`	your policy withdrew that device's AI access
`ungoverned_agent.access_restored`	access came back, because the agent was removed

Only the transitions are sent. A device that has had the same agent for a week produces one event, not one every thirty seconds.

The event names the agent and the specific risks found — including `openclaw.lethal_trifecta`, which means one agent has host command execution, access to private data, and a channel to the outside world at the same time. That is the one to alert on.

Administrator actions

Every change an administrator makes in the console, as an **OCSF Entity Management (3004)** event: policy changes, API credentials created or revoked, devices revoked, developers invited and offboarded, provider keys, SSO configuration, alert channels, and changes to the SIEM destination itself.

Each says who did it (name and email), what they changed, and what the new value is.

Worth a rule of its own: `siem_destination.updated` and `siem_destination.deleted` mean somebody changed where your audit evidence goes.

Failed attempts are not recorded as changes — a rejected request changed nothing, and an audit log listing things that never happened is worse than one that omits attempts.

What we never send

- **Prompt and response content.** Events are metadata. Captured conversations, if you enable them, stay in Sentilai and are never part of this stream.
- **The secret itself.** A finding tells you an AWS key was present and how many times — never the key.
- Provider API keys, tokens, or credentials of any kind.

Revision #2
Created 2026-08-04 08:39:24 UTC by Sentilai Docs
Updated 2026-09-29 14:39:20 UTC by Sentilai Docs