SIEM: pull with the OCSF API

The pull option: your SIEM asks Sentilai for events on its own schedule.

The endpoint

`GET /api/siem/v1/events?cursor=&limit=1000`

Events are in **OCSF** — the Open Cybersecurity Schema Framework — so they land in a shape Splunk, Microsoft Sentinel, Elastic and QRadar already understand.

Authentication

An **API credential** with the `audit:read` scope. Create it on **API Credentials**; the secret is shown exactly once.

Give this credential only `audit:read`. It is going to live in a configuration file in another system, and it should be able to do nothing except read audit events.

Cursor pagination

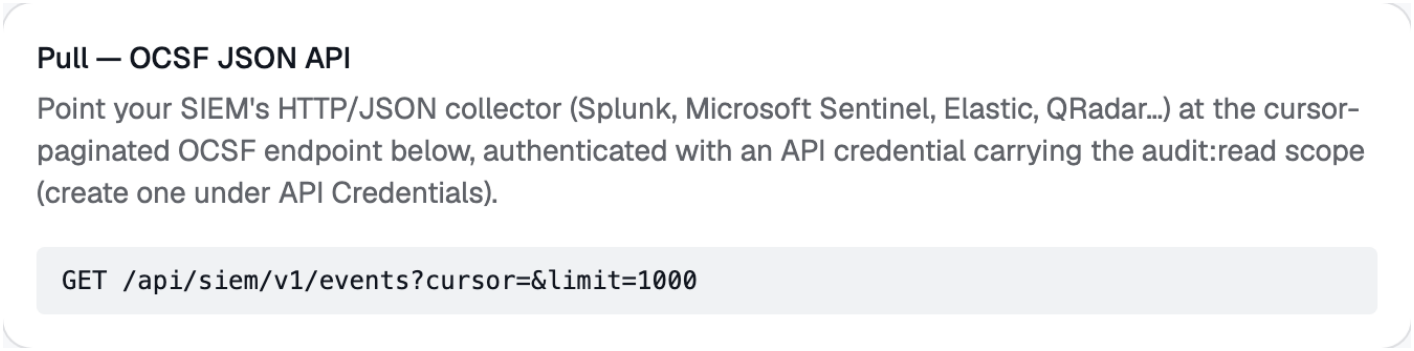
Each response carries a cursor. Store it, pass it next time, get what has happened since. This is what makes the integration resumable: a SIEM that was down for a day catches up rather than losing the gap.

Choosing pull or push

Pull is more reliable — your SIEM controls the pace and can retry. It is the default recommendation.

Push is lower-latency and suits SIEMs that prefer to receive syslog. See *SIEM: push over syslog*.

You can run both.



The pull card on SIEM Export — the OCSF endpoint, and the one-scope credential it needs.

Revision #12
Created 2026-08-02 10:19:36 UTC by Sentilai Docs
Updated 2026-09-29 14:39:19 UTC by Sentilai Docs