SIEM and alerts are not arriving

Push delivery stopped

SIEM Export shows delivered count, last success, last attempt and **last error**. Start there — it usually names the cause: an expired certificate, a moved collector, a closed port.

The status badge reads **Active** or **Paused**.

Push was never configured correctly

Private and internal hostnames are rejected — the collector must be reachable from Sentilai, so a `10.x` address will not work. Either publish the collector on a name we can reach, or use the pull API from inside your network.

Send test event delivers a `siem_push_test`. If that does not arrive, nothing else will.

Pull returns nothing

Check the credential has **`audit:read`**, has not expired, and is not blocked by its own IP allowlist. The **Last used** column on API Credentials tells you whether your calls are arriving at all.

Check you are passing the **cursor** back. Without it you re-read the same page forever.

Alerts stopped arriving

Alerts are **fire-and-forget** — delivery is attempted alongside the request and never blocks it, which means an alert can be lost if the destination is briefly unreachable.

Use **Send test** on the channel. If the test arrives and real alerts do not, check the channel's **minimum severity**: "High only" will stay silent through a great deal of genuine medium-severity activity.

If you need guaranteed delivery of every event, that is the SIEM path, not alerts.

Revision #6
Created 2026-08-02 10:20:20 UTC by Sentilai Docs
Updated 2026-08-04 08:40:01 UTC by Sentilai Docs