What alerts are for

The delivery guarantee

Alerts are **fire-and-forget**. Delivery is attempted alongside the request, never in front of it: a Slack outage cannot slow down or fail your developers' AI traffic. The trade-off is that an alert can be lost if the destination is unreachable, so alerts are a notification mechanism and not an audit trail.

The audit trail is Activity, Compliance and your SIEM. If you need guaranteed delivery of every event, use Stream events to your SIEM — that path is built for completeness. Alerts are built for attention.

What to route where

- **Slack or Teams** for the things a human should look at today: high-severity classifier verdicts, secrets blocked, a lethal-trifecta block.
- **A generic webhook** when you want to drive something automatic — open a ticket, page someone, tag a device in your own tooling.

Multiple channels

You can have several, each with its own severity threshold. A common arrangement is a noisy engineering channel at "Medium and up" and a quiet security channel at "High only".

What not to do

Do not use alerts as your compliance evidence. When an auditor asks what happened in March, the answer comes from the evidence pack on **Compliance**, not from a Slack channel with a 90-day history and no guarantee of completeness.

Revision #8
Created 2026-08-02 10:20:08 UTC by Sentilai Docs
Updated 2026-08-02 16:30:36 UTC by Sentilai Docs