



FLOWMATRIX.DEV

Premium Workflow

A practical guide – step by step

Partner API Monitoring

Monitor partner API health, detect failures early and alert the team with useful context.

ENGINEERING

INTERMEDIATE

ABOUT 2 HOURS SETUP

OVERVIEW

Partner API Monitoring

Monitor partner API health, detect failures early and alert the team with useful context.

CATEGORY	DIFFICULTY	DURATION
Engineering	Intermediate	About 2 hours setup

What you use it for

Early warning for third-party API outages.

Tools in this workflow

Cloudflare Workers API · PostHog Analytics API · Slack · Supabase

How to implement it

1

Define critical partner endpoints

List the partner APIs your product depends on and the expected response times.

WHAT YOU NEED TO DO

1. Write down every critical endpoint.
2. Define a timeout and success status.
3. Set a warning threshold per endpoint.
4. Store the list in Supabase.

CHECK AT THE END

- ☐ All critical endpoints are listed
- ☐ Thresholds are documented

RESULT

A monitored endpoint inventory exists.

LINKS

Supabase Database Guide: <https://supabase.com/docs/guides/database>

2

Run scheduled health checks

Use a scheduled worker to call each endpoint and record the result.

WHAT YOU NEED TO DO

1. Create a Cloudflare Worker with a cron trigger.
2. Send a lightweight request to each endpoint.
3. Record status code and latency in Supabase.
4. Store the error message when a call fails.

CHECK AT THE END

- ☐ Cron trigger runs on schedule
- ☐ Latency is stored for every call

RESULT

Health check results are collected continuously.

LINKS

Cloudflare Cron Triggers: <https://developers.cloudflare.com/workers/configuration/cron-triggers/>

3

Detect incidents

Compare recent results with the threshold and open an incident when needed.

WHAT YOU NEED TO DO

1. Query the last ten results per endpoint.
2. Mark an incident after three failures.
3. Avoid duplicate incidents for the same cause.
4. Close the incident after three successes.

CHECK AT THE END

- ☐ Three failures open an incident

[] Three successes close it

RESULT

Incidents open and close automatically.

LINKS

Cloudflare Workers Docs: <https://developers.cloudflare.com/workers/>

4

Send context-rich alerts

Alert the team with the endpoint, error and recent latency trend.

WHAT YOU NEED TO DO

1. Post the incident to a Slack channel.
2. Include the last error message.
3. Add a link to the PostHog dashboard.
4. Mention the owning team.

CHECK AT THE END

- ☐ Alert includes the endpoint
- ☐ Owning team is mentioned

RESULT

The team can start investigating immediately.

LINKS

PostHog API: <https://posthog.com/docs/api>

5

Review incidents monthly

Look for recurring partner issues and adjust timeouts or fallbacks.

WHAT YOU NEED TO DO

1. List incidents from the last month.
2. Group them by partner and error type.
3. Adjust thresholds for noisy endpoints.
4. Document partner risks for the next review.

CHECK AT THE END

- ☐ Monthly review is scheduled
- ☐ Noisy alerts are tuned

RESULT

Monitoring stays useful and low-noise.

LINKS

PostHog Documentation: <https://posthog.com/docs>

RECOMMENDED TOOLS & RESOURCES

Recommended Tools & Resources

All tools in this workflow with their official website.

Cloudflare Workers API

<https://workers.cloudflare.com/>

PostHog Analytics API

<https://posthog.com/>

Slack

<https://slack.com/>

Supabase

<https://supabase.com/?ref=flowmatrix>

Official URL

Full version as Premium PDF

All steps, tools and resources as a PDF – €4.99.

[Buy now – €4.99](#)