ProjectX

INCIDENT RESPONSE WITH APPROVALS · USE-CASE BRIEF

One alert queue for everything, and a response that waits for a person where it should.

Alerts from identity, data, video, cloud and the platform in one model and one severity scale, grouped into incidents with an owner and an SLA, worked by a responder agent whose risky steps wait for approval, and closed with a review that links the evidence.

The situation

A camera goes dark, a finance account signs in from a new country and a pipeline falls behind, in three tools with three paging rules. The on-call engineer pieces it together at 3 a.m. and the post-mortem is a document nobody finds again.

How it works, step by step

01 **One queue across pillars** · Operational Intelligence
Every pillar's alerts share one model and one severity scale, and repeats are folded by dedupe key.

02 **Group it into an incident** · Operational Intelligence
Related alerts correlate into an incident with an owner, an SLA and an escalation policy with on-call rotation.

03 **Respond with a workflow** · Workflows & Agents
A workflow notifies, opens a case and contains access, each action authorized as the person who triggered it.

04 **Let the responder agent help** · Workflows & Agents
The ops responder reads alerts, acknowledges and assigns, and can run a remediation; risky steps wait for approval.

05 **Review and learn** · Operational Intelligence
A structured review links the evidence, and analytics report volume, precision, MTTA and MTTR by source.

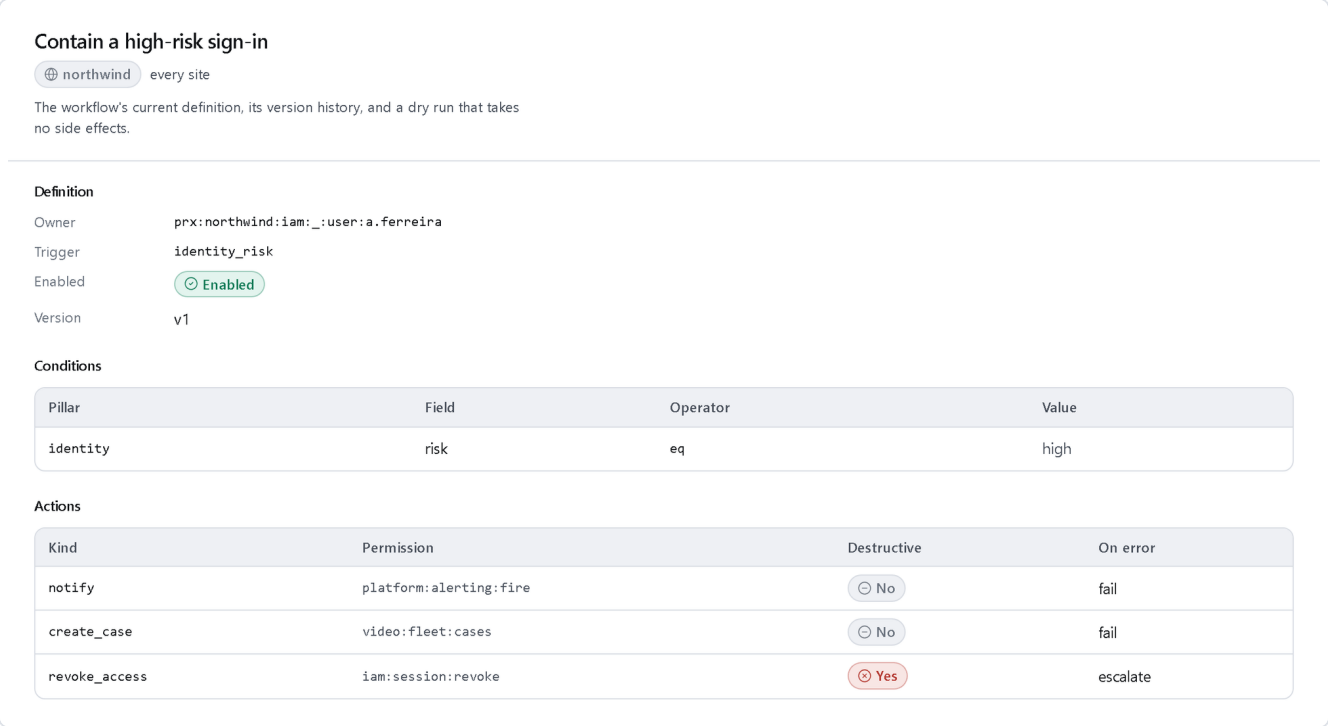
What you get

01
One place to look
Every pillar's alerts in one queue, ranked on one scale.

02
Speed without blind automation
Workflows and agents act fast, and destructive steps still wait for a person.

03
Response times you can measure
MTTA and MTTR by source, from the same records the incident was worked in.

In the console



Trigger, condition and actions, each with the permission it needs. Screens shown with demo data.

Questions buyers ask

Does it page our existing tools?
Yes. Connectors reach PagerDuty and Opsgenie, Slack and Teams, and ServiceNow and Jira Service Management.

Can we try a workflow without it acting?
A dry run plans and authorizes every step as a real run would, and takes none of them.