

Visa cut triage on a high-stakes mainframe alert from 10–20 minutes to seconds

Visa's first Elastic Security workflow performs the investigation's repeatable first steps automatically, using a controlled, auditable AI step to hand incident response to a case that is ready for decision. The pattern is now reusable across other detections.

Min → sec

Per-fire triage time

0

Analyst pivots before IR

1st

Reusable pattern at Visa

1

Native platform, no bolt-on SOAR

The challenge

- ✗ A high-stakes mainframe identity detection fired in the legacy SIEM, but the alert named the event, not the person.
- ✗ Incident response had to log in and run a second search to identify the user.
- ✗ The speed and quality of that work varied sharply with analyst experience.
- ✗ Every fire cost 10–20 minutes of manual context-gathering before investigation could even begin.

The solution

- ✓ A four-stage Elastic workflow automates the investigation's repeatable first steps and hands IR a summarized case.
- ✓ A narrow AI step verifies the finding and writes the summary; it never decides whether to escalate.
- ✓ Every decision is anchored in team-controlled data, the prerequisite for trusting AI in a regulated environment.
- ✓ It runs natively in Elastic, so there's no separate orchestration platform to maintain.

How the workflow runs

1. Ingest & normalize

Find the flagged activity

2. Detect & correlate

Identify the user behind it

3. Triage & investigate

AI verifies and summarizes

4. Respond & report

A ready case opens in IR

Before

- Raw event, then a manual second search in a separate tool
- 10–20 min per fire; quality varied by analyst skill
- Work split across the legacy SIEM and a separate orchestration tool

After

- An enriched, summarized case arrives in IR ready to decide
- Seconds end to end; consistent regardless of who is on shift
- One native workflow, with no separate platform to maintain

“What used to require 10 to 20 minutes of analyst effort per fire now completes in **seconds**. The IR team is receiving a **fully contextualized alert** that is ready for decision-making.”

— Visa Cybersecurity Engineering team

Why it matters beyond one alert

The detection fires only a few times a year; it was chosen because the per-fire cost was clearly worth eliminating and the four-stage shape is portable. Anywhere a detection needs a known, repeatable follow-up before an analyst can act, the same pattern applies. Visa's separate automation team has already requested access to Elastic, opening a path to consolidate response onto a single platform, and the team is now evaluating Attack Discovery as the next step.