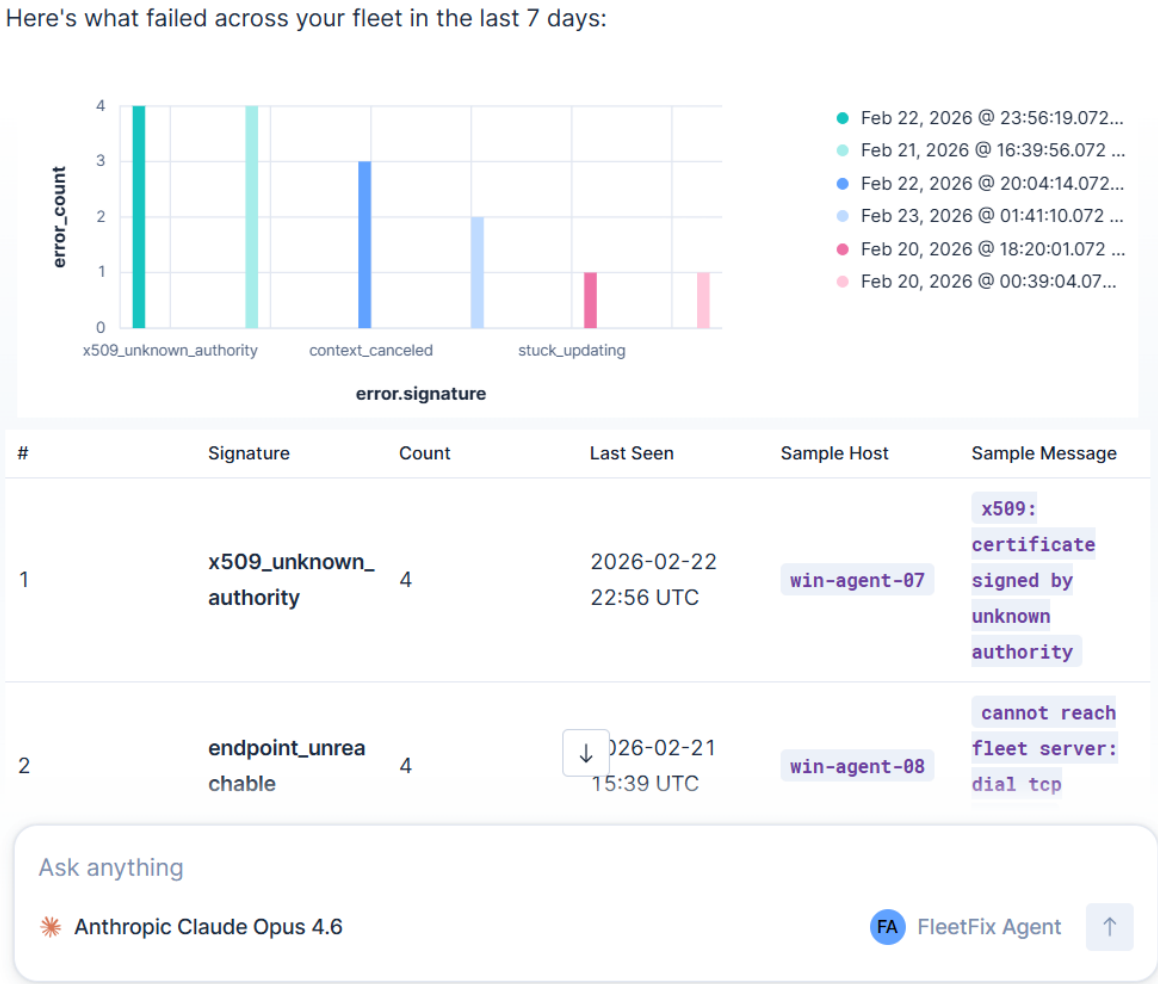
FleetFix Agent

Ops triage + runbooks + ticket creation
(Elastic Agent Builder + Elasticsearch)

- Detect the top Fleet/Agent failures (cluster by signature)
- Retrieve the exact runbook (fix + verify steps)
- Create a tracking ticket via workflow (with confirmation)



Problem

Fleet / Elastic Agent failures are repetitive and time-consuming:

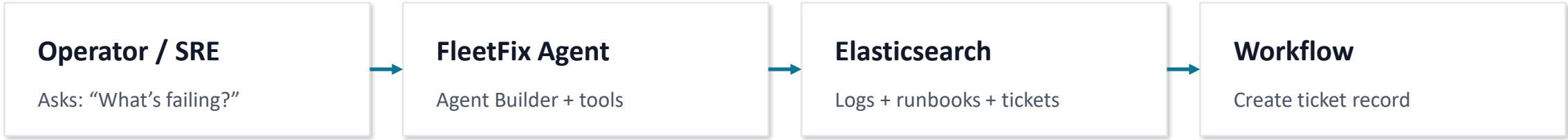
Before

- Same errors recur across many hosts (e.g., enrollment, TLS, policy timeouts)
- Triage requires hopping between logs, docs, and tribal knowledge
- Fix steps are inconsistent → slow resolution and repeat incidents

After (FleetFix)

- Clusters failures by signature and shows the top issues
- Pulls the exact runbook (root causes, fix steps, verification)
- Creates a ticket record with recommended steps (via workflow)

How it works



FleetFix tools

- detect_failure_clusters (ES|QL): top signatures + sample host/message
- search_runbooks (Index search): natural-language search over runbooks
- get_runbook_by_signature (ES|QL): exact runbook lookup
- create_ticket (Workflow): writes to fleetfix_tickets with confirmation

Live demo

1) Detect top failures

Prompt: “What are the top Fleet failures in the last 24 hours?”

Expected outcome

Shows clustered signatures with counts + sample host/message.

2) Pull the runbook

Prompt: “Get runbook for context_canceled”

Expected outcome

Returns root causes + fix steps + verification steps.

3) Track it (safe action)

Prompt: “Create a ticket for context_canceled on win-agent-01, severity high.”

Expected outcome

Agent asks for confirmation → workflow writes a ticket doc.