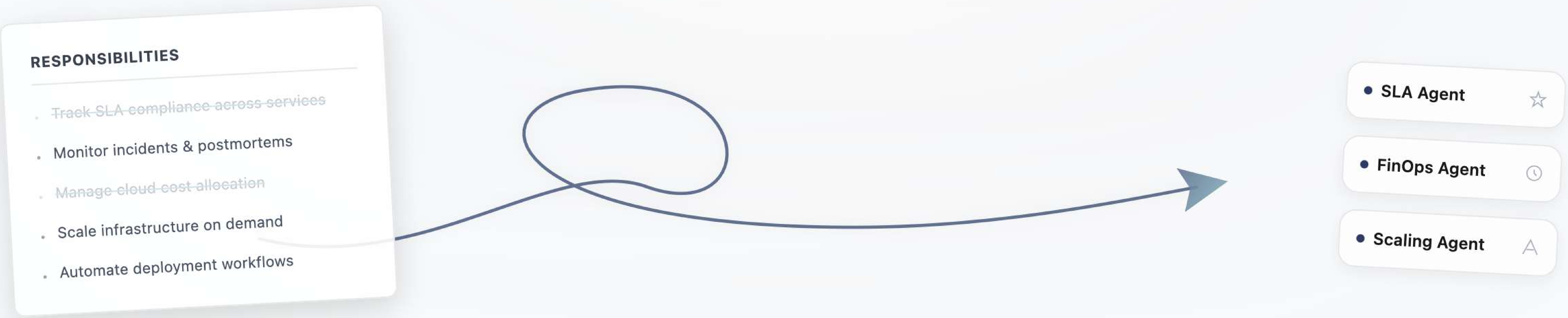
CloudShip

Turning DevOps responsibilities into Agents



RESPONSIBILITIES

- ~~Track SLA compliance across services~~
- Monitor incidents & postmortems
- ~~Manage cloud cost allocation~~
- Scale infrastructure on demand
- Automate deployment workflows

- SLA Agent ☆
- FinOps Agent
- Scaling Agent

Our Mission

Teams want to adopt AI internally, but there's no secure way to do it for their operations

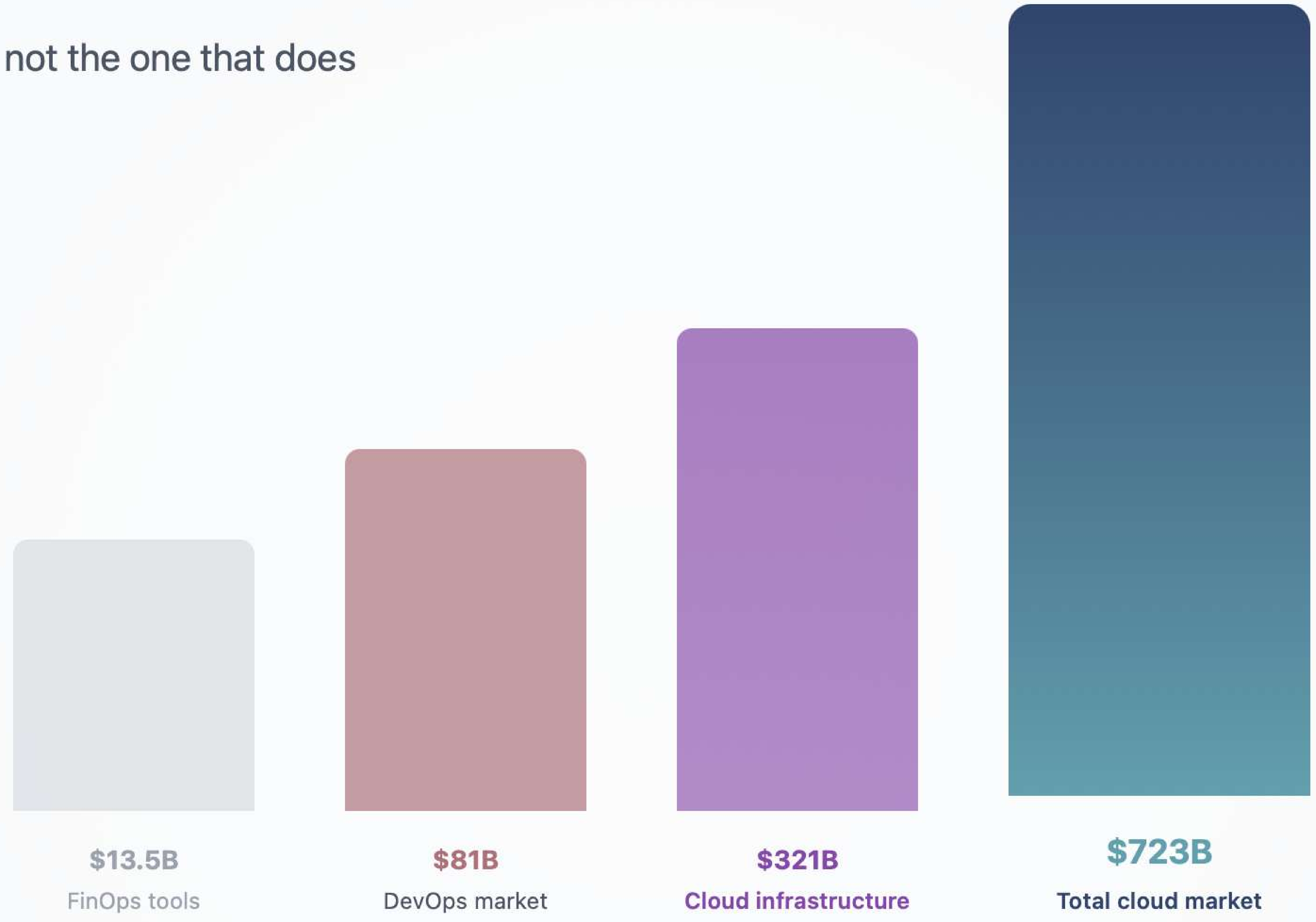
PROBLEM Teams want to adopt AI internally, but there's no secure way to do it for their operations.

SOLUTION We're building AI agents that operate infrastructure autonomously with full visibility and control.

VISION **From manual operations to autonomous infrastructure.**

Building for the future

Building for the org chart that will exist, not the one that does



Traditional

👤 → 👤 👤 → 👤 👤 👤

Scale = Headcount

2026

👤 + Agent Layer = 🚀

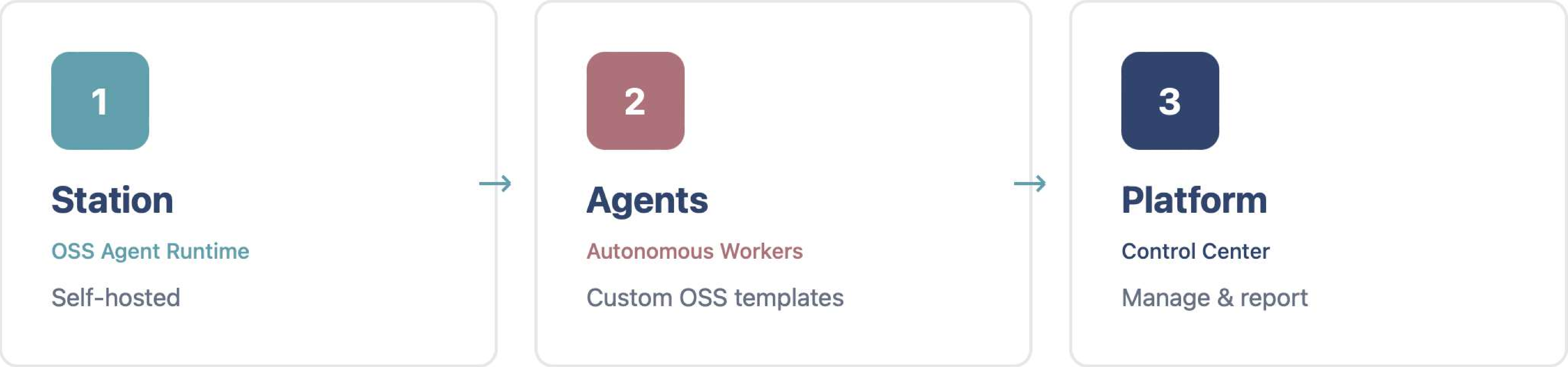
Scale = Agents

Every company becomes a tech company. Every team becomes agent-powered.

Sources: MarketsandMarkets Cloud FinOps 2024 ($13.5B),
IMARC DevOps Market 2024 ($81B by 2033),
Canalys Cloud Infrastructure 2024 ($321B),
Gartner Public Cloud Forecast 2025 ($723B)

The CloudShip Suite

The framing and infrastructure for how teams and DevOps agents work together securely



1 **Station**
OSS Agent Runtime
Self-hosted

→

2 **Agents**
Autonomous Workers
Custom OSS templates

→

3 **Platform**
Control Center
Manage & report

Connect
Your infra

Execute
24/7 agents

Report
ROI & insights

Our Approach

Purpose-built for teams permissions

1 Model Freedom

*Companies like **JPMorgan** can only use their HIPAA-approved Claude instances*

🏦 Banks = FedRAMP certified 🏥 Healthcare = HIPAA approved 💊 Pharma = Validated models 🛡️ Defense = Air-gapped

2 Zero Credentials

*Companies like **Stripe** will not give AWS credentials to cloud agents (prompts they don't see)*

🚫 FinTech = No AWS keys 🔐 SaaS = No DB passwords 📊 Everyone = Telemetry only 👁️ Logs not credentials

3 Stack Agnostic

*Companies like **Netflix** run AWS for compute, Azure for apps, GCP for analytics*

☁️ Cloud = AWS+Azure+GCP 🗄️ Data = Postgres+Mongo 🔧 Code = GitHub+GitLab 🌐 Reality = Heterogeneous

4 Prompt Freedom

*Companies like **Goldman Sachs** fear AI vendor lock-in from closed prompts*

📖 Prompts = MIT licensed 🔓 Code = Open source 🏔️ Moat = Cloud insights 🆓 IP = Free forever

Every "no" we heard became a design decision

The Pattern Repeats

We see what competitors miss

Company	Their Insight	What Won	Beat
Kubernetes	Teams needed centralized control over distributed containers	Fine-grained RBAC	~~Docker Swarm basic permissions~~
GitLab	Teams will not manage permissions across 8+ security tools	Built-in security scanning	~~Tool sprawl~~
HashiCorp Vault	Teams will not scatter AWS keys across config files and env vars	Centralized secrets management	~~Scattered credential files~~
CloudShip	Teams will not give credentials to cloud agents they do not control	**Local-first OSS agent templates**	~~Cloud agents~~

sabo2205 • 1y ago

I don't need it because our infrastructure mostly run on ECS Fargate and Lambda. Plus our resources spread across **multiple accounts so 1 credential will not do it.**

Exposing credential to third party is a no no for me too.

ivix • 2y ago

No offence, but **you have no business giving your AWS access key to anybody** if you don't understand anything about what is going on.

This is not like playing around on some social media app. **AWS is a professional tool, and you can get into serious trouble.**

CSYVR • 1y ago

any tool that requires plain access credentials is immediately disqualified for my use. most organizations use **AWS sso with short lived credentials** and even go as far as preventing iam users from being created.

if you really think the plugin is worth it, **spend some time on getting the access part right.** when a user is logged in to the console, there are temporary credentials in the browser store that you might be able to use

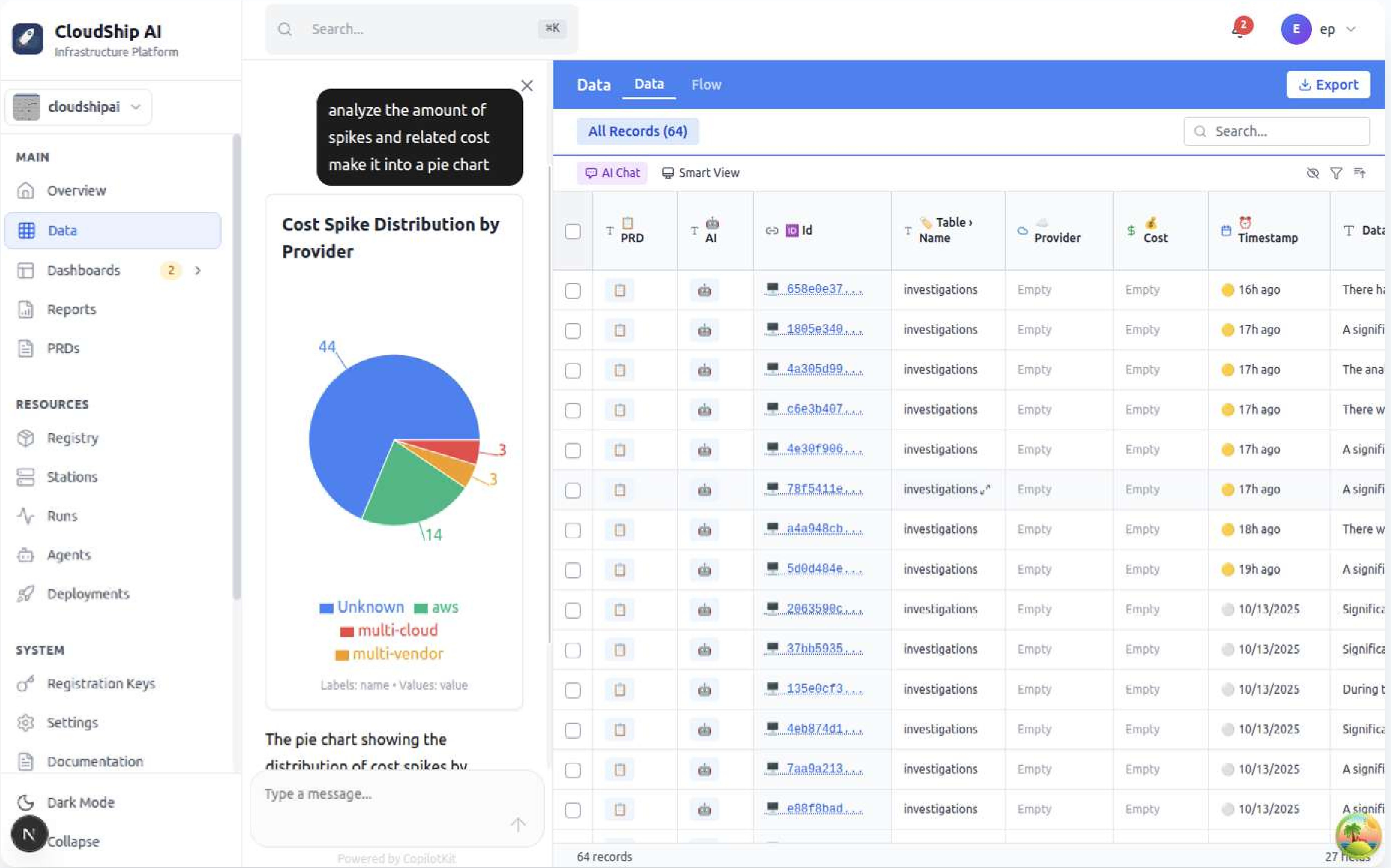
The pattern is clear. Centralized control wins every time.

The CloudShip Platform

Where agent outputs become insights

- Single pane of glass for all agent activity
- AI understands your infrastructure context
- Automatic ROI tracking & reporting
- RBAC & team management
- Manage and share prompts, agents, and tools through the platform while they run on your own infrastructure and we see no credentials

Each agent knows its job. Platform knows everything.



analyze the amount of spikes and related cost make it into a pie chart

Cost Spike Distribution by Provider

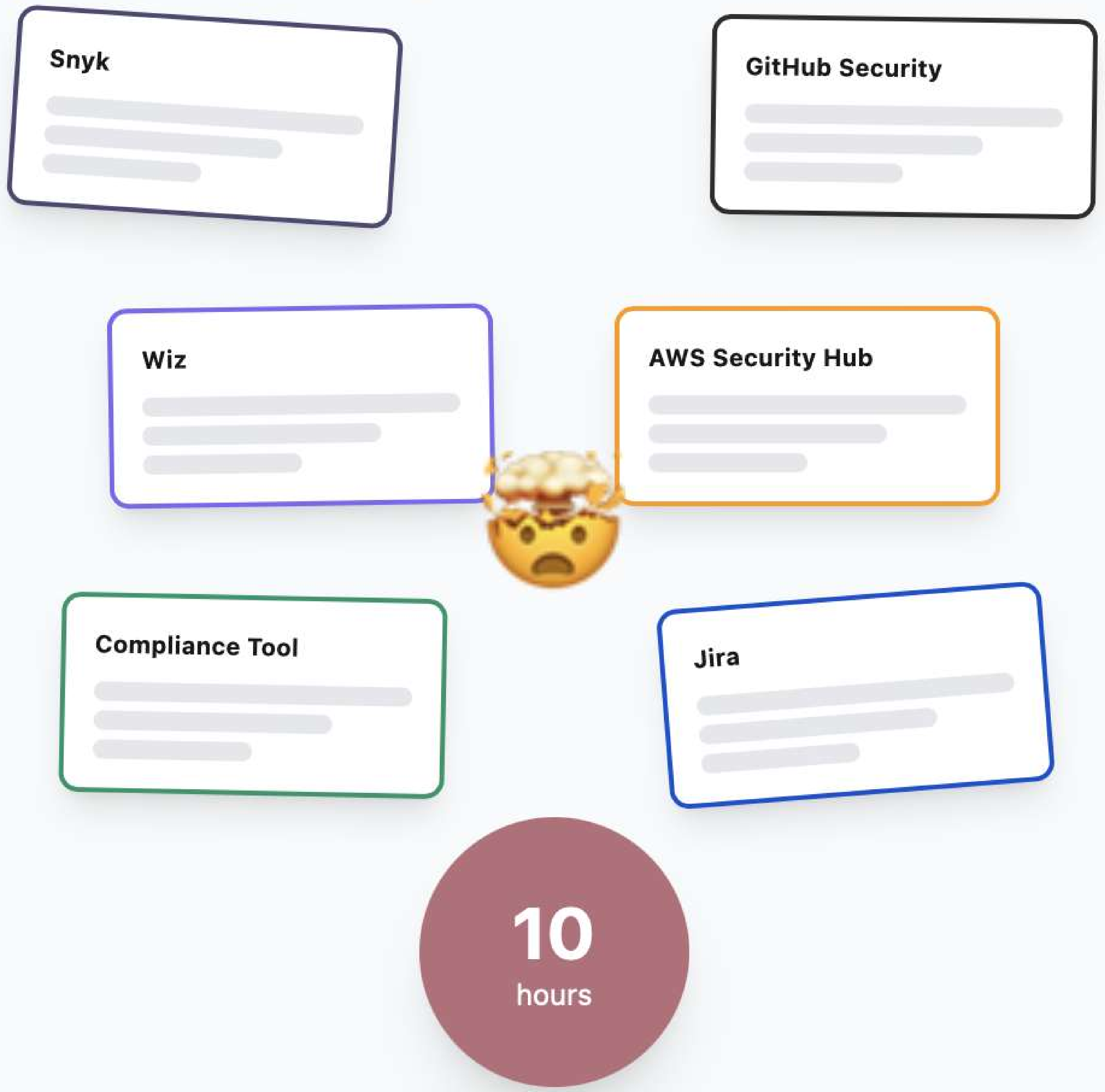
The pie chart showing the distribution of cost spikes by

□	PRD	AI	Id	Table › Name	Provider	Cost	Timestamp	Data
□			658e0e37....	investigations	Empty	Empty	16h ago	There h
□			1805e340....	investigations	Empty	Empty	17h ago	A signifi
□			4a305d99....	investigations	Empty	Empty	17h ago	The ana
□			c6e3b407....	investigations	Empty	Empty	17h ago	There w
□			4e30f906....	investigations	Empty	Empty	17h ago	A signifi
□			78f5411e....	investigations	Empty	Empty	17h ago	A signifi
□			a4a948cb....	investigations	Empty	Empty	18h ago	There w
□			5d0d484e....	investigations	Empty	Empty	19h ago	A signifi
□			2063590c....	investigations	Empty	Empty	10/13/2025	Significa
□			37bb5935....	investigations	Empty	Empty	10/13/2025	Significa
□			135e0cf3....	investigations	Empty	Empty	10/13/2025	During t
□			4eb874d1....	investigations	Empty	Empty	10/13/2025	Significa
□			7aa9a213....	investigations	Empty	Empty	10/13/2025	A signifi
□			e88f8bad....	investigations	Empty	Empty	10/13/2025	A signifi

64 records 27 fields

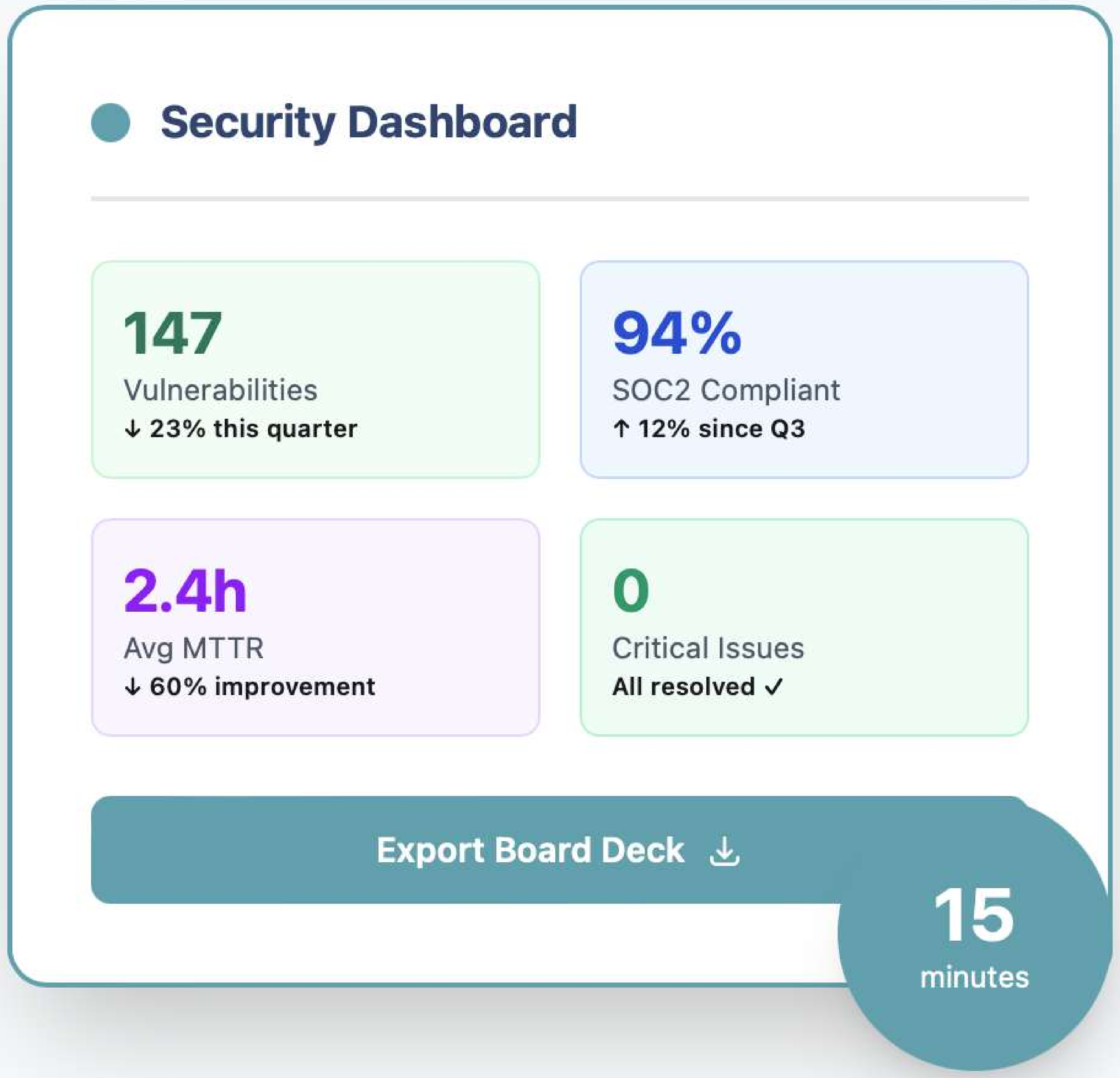
Use Case: Security Metrics for the Board

Prove your security program is working



Security Tool Sprawl

Login 6 times. Export 6 CSVs. Pray Excel doesn't crash.



Security Dashboard

147 Vulnerabilities ↓ 23% this quarter	94% SOC2 Compliant ↑ 12% since Q3
2.4h Avg MTTR ↓ 60% improvement	0 Critical Issues All resolved ✓

Single Source of Truth

All tools unified. Real-time metrics. One-click export.

10 hours → 15 minutes. Live data, not stale reports. Board sees you're in control.

Appendix: Security Metrics Agent

Unified dashboard for board reporting

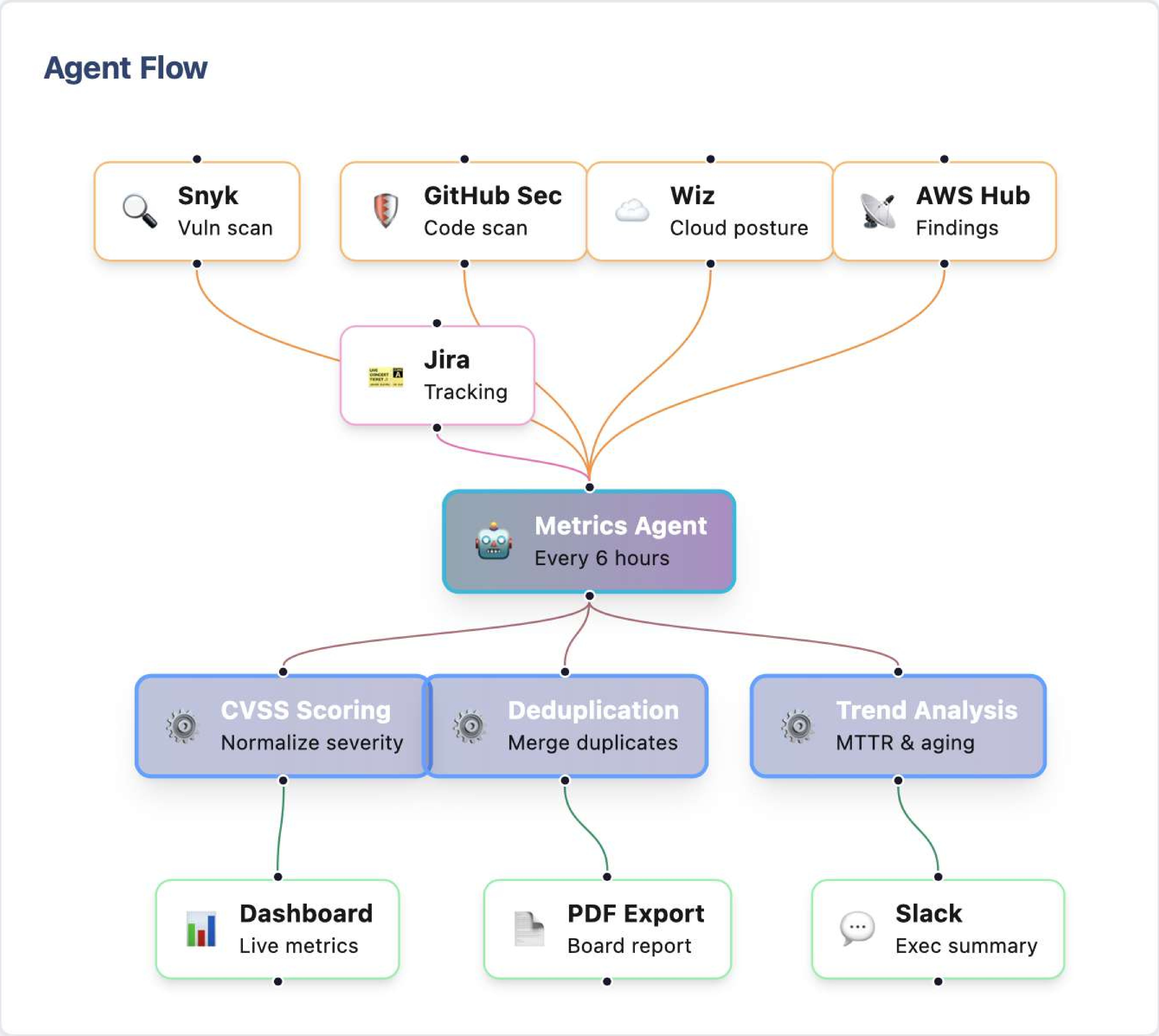
station.yml

```yaml
---
metadata:
  name: "Security Metrics Aggregator"
  description: "Unify 6 security tools → single board-read
model: gpt-4o-mini
max_steps: 8
tools:
  - "__snyk"              # Vuln scanning (750+ policies)
  - "__github_security"   # Code scanning & Dependabot
  - "__wiz"               # Cloud security posture
  - "__aws_security_hub"  # AWS security findings
  - "__jira"              # Ticket resolution tracking
  - "__slack"             # Executive summaries
---

{{role "system"}}
You are a security metrics analyst specializing in vulnera
Aggregate security metrics from fragmented tools into a un

{{role "user"}}
{{userInput}}
```

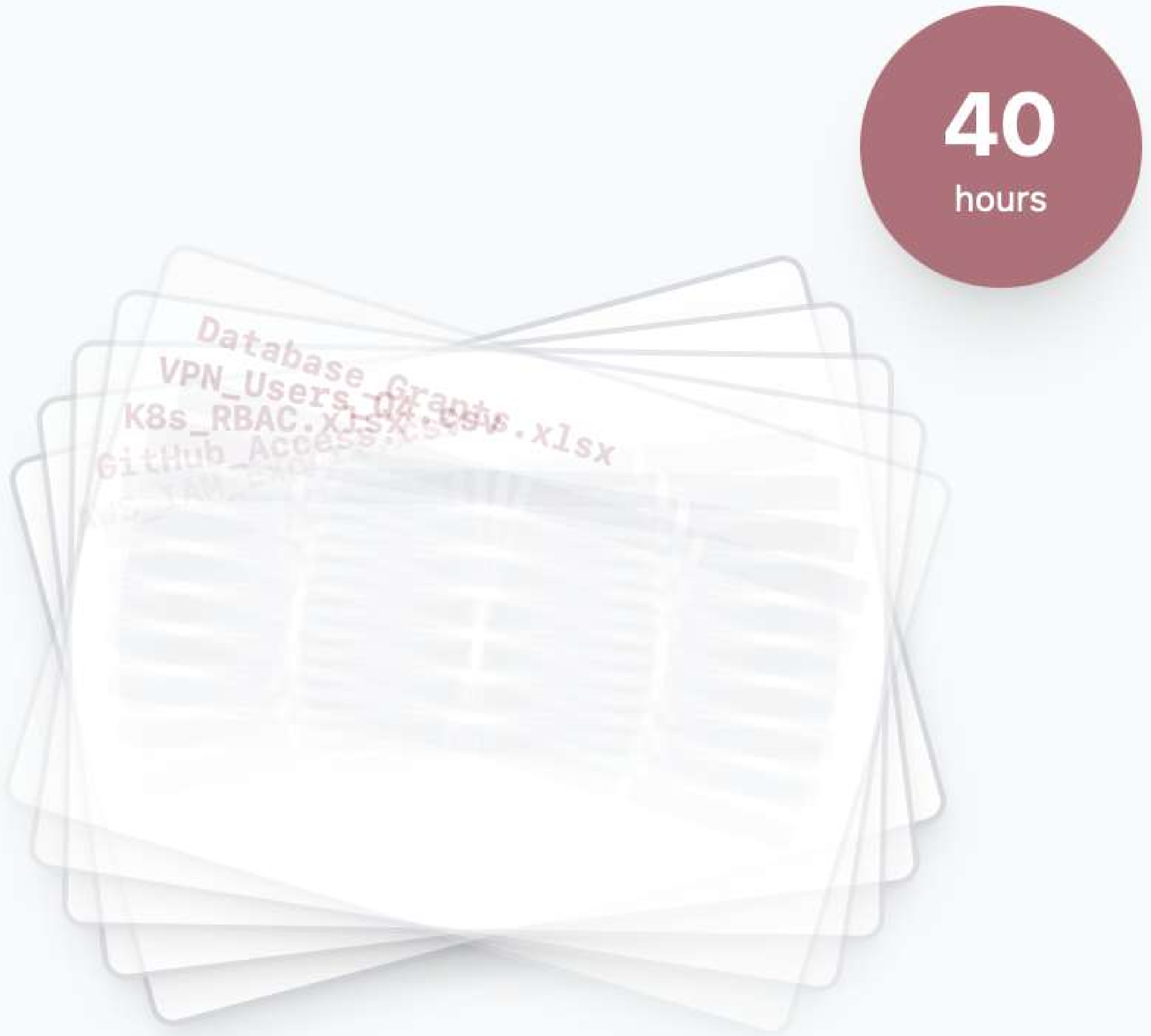
Agent: `security-metrics-aggregator`

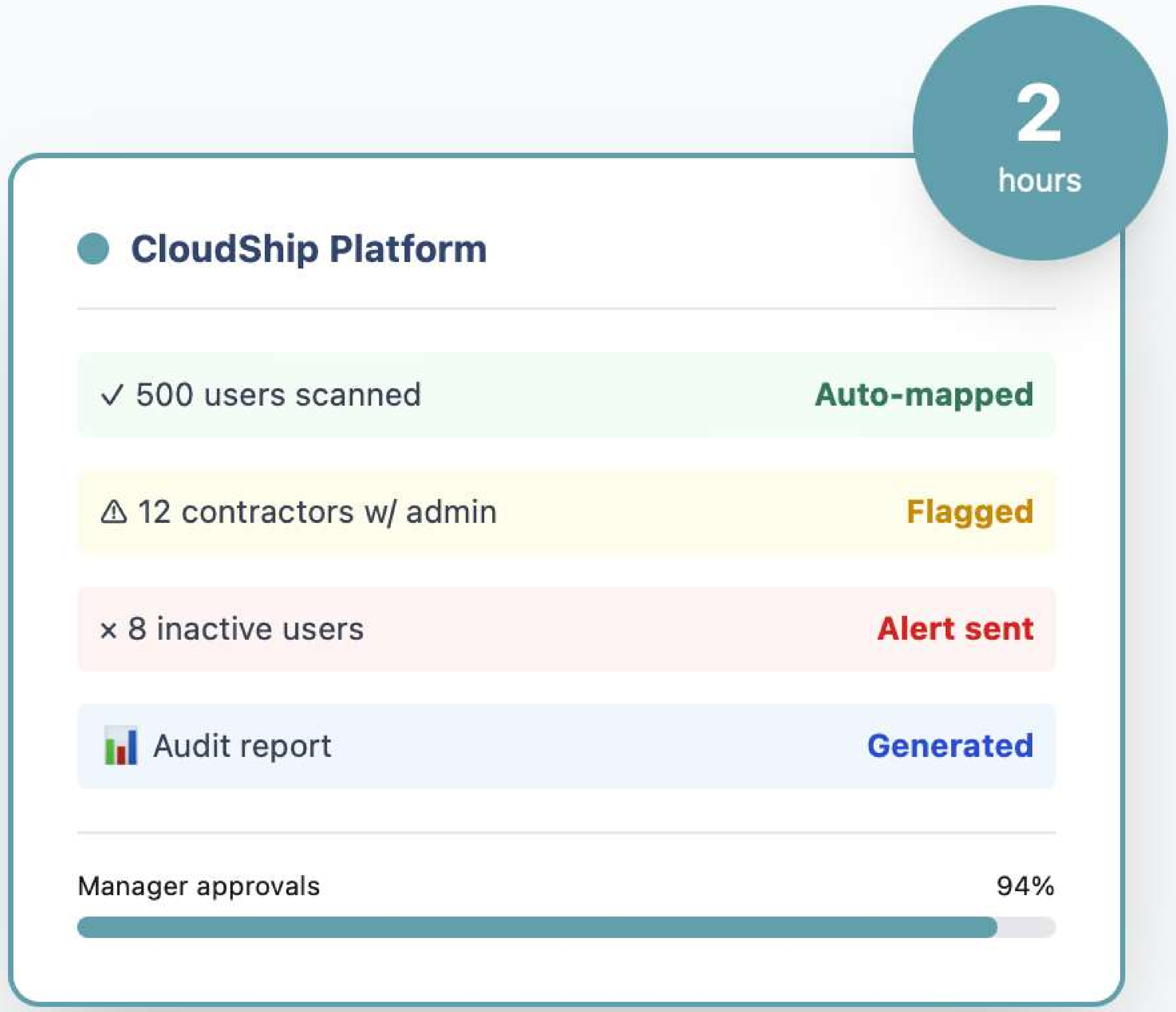


Runs in your infrastructure. Credentials never leave your environment.

Use Case: Quarterly Access Reviews

Required for SOC2, ISO27001, and PCI compliance





● **CloudShip Platform**

✓ 500 users scanned **Auto-mapped**

⚠ 12 contractors w/ admin **Flagged**

× 8 inactive users **Alert sent**

📊 Audit report **Generated**

Manager approvals 94%

Manual Spreadsheet Hell

50+ systems → 50+ exports → 1 merged nightmare

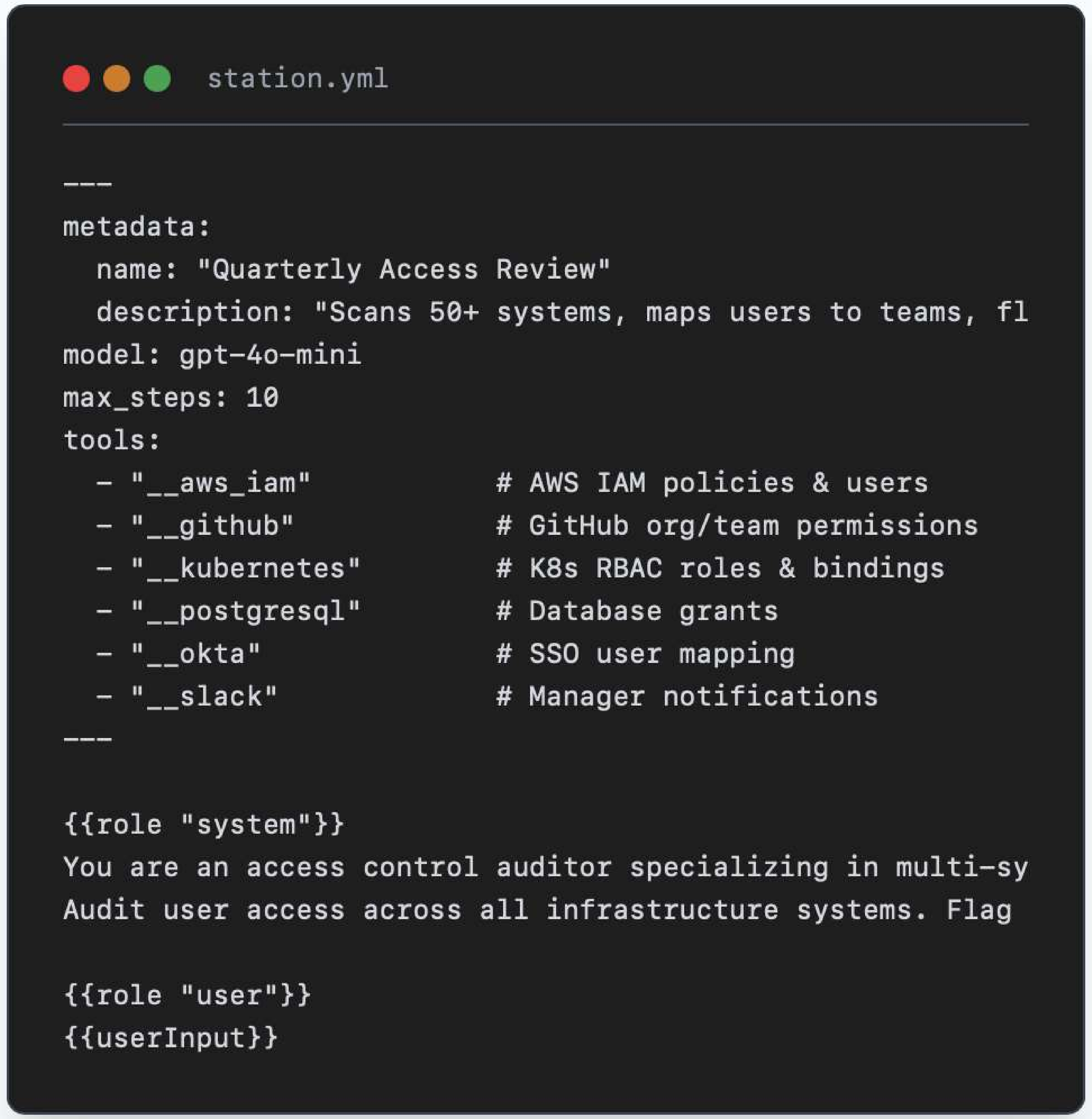
Automated Across All Systems

One click. Real-time sync. Zero spreadsheets.

40 hours → 2 hours. Complete audit trail. Zero spreadsheets.

Appendix: Access Review Agent

How it works under the hood



station.yml

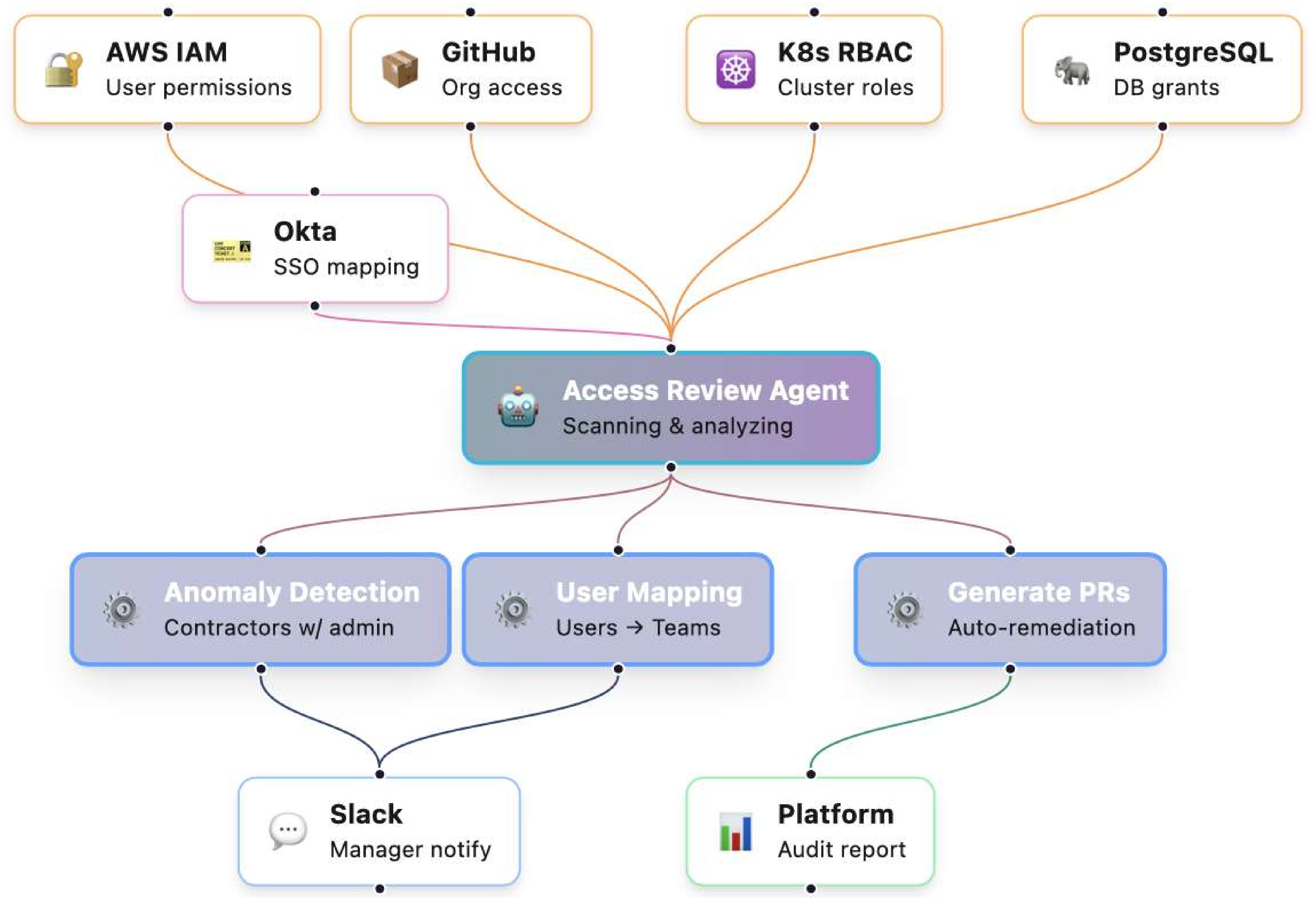
```
---
metadata:
  name: "Quarterly Access Review"
  description: "Scans 50+ systems, maps users to teams, fl
model: gpt-4o-mini
max_steps: 10
tools:
  - "__aws_iam"           # AWS IAM policies & users
  - "__github"            # GitHub org/team permissions
  - "__kubernetes"        # K8s RBAC roles & bindings
  - "__postgresql"        # Database grants
  - "__okta"              # SSO user mapping
  - "__slack"             # Manager notifications
---

{{role "system"}}
You are an access control auditor specializing in multi-sy
Audit user access across all infrastructure systems. Flag

{{role "user"}}
{{userInput}}
```

Agent: `access-review-agent`

Agent Flow



AWS IAM
User permissions

GitHub
Org access

K8s RBAC
Cluster roles

PostgreSQL
DB grants

Okta
SSO mapping

Access Review Agent
Scanning & analyzing

Anomaly Detection
Contractors w/ admin

User Mapping
Users → Teams

Generate PRs
Auto-remediation

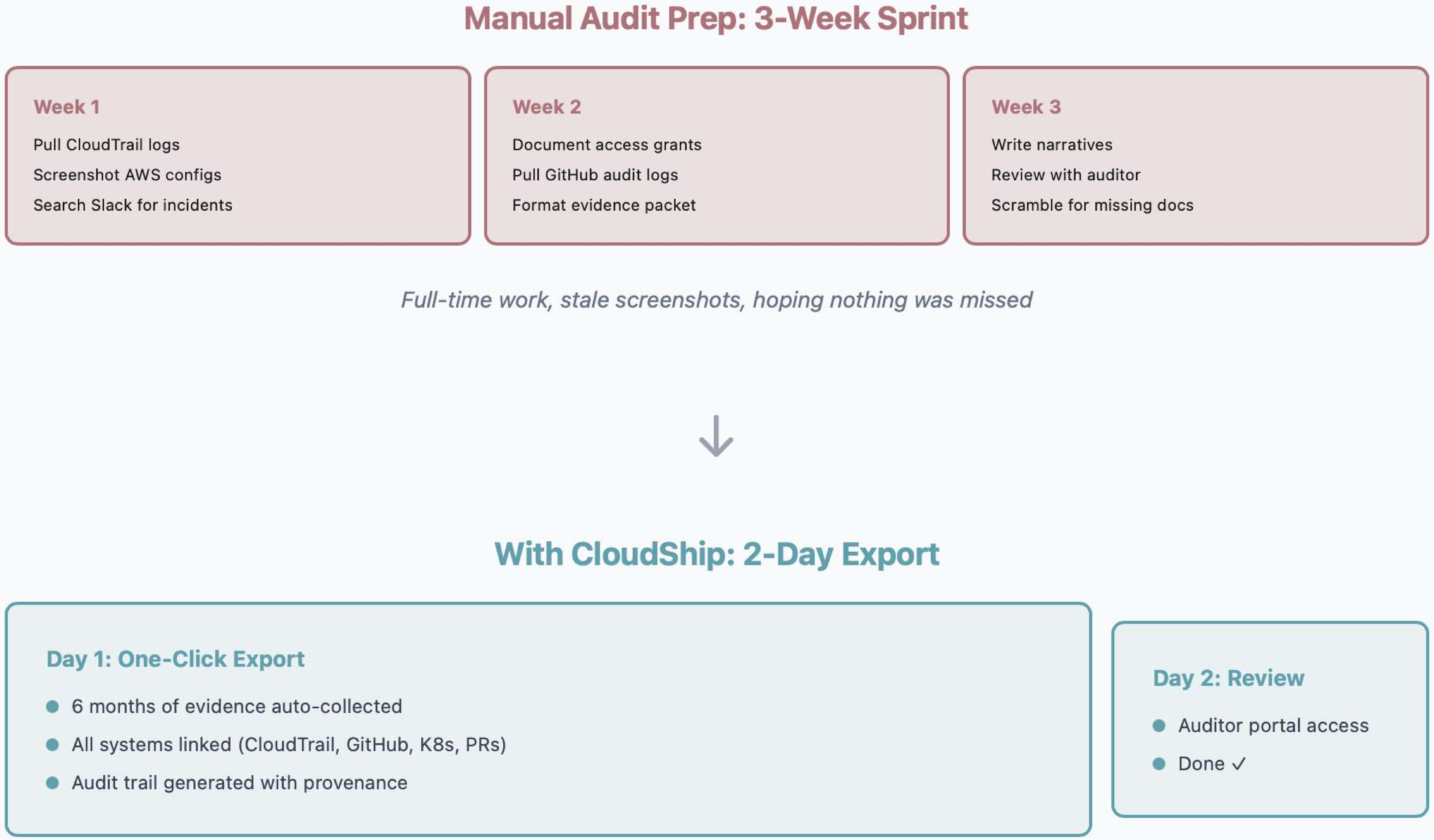
Slack
Manager notify

Platform
Audit report

Runs in your infrastructure. Credentials never leave your environment.

Use Case: SOC2 Audit Prep

Continuous compliance evidence collection



Manual Audit Prep: 3-Week Sprint

Week 1
Pull CloudTrail logs
Screenshot AWS configs
Search Slack for incidents

Week 2
Document access grants
Pull GitHub audit logs
Format evidence packet

Week 3
Write narratives
Review with auditor
Scramble for missing docs

Full-time work, stale screenshots, hoping nothing was missed

↓

With CloudShip: 2-Day Export

Day 1: One-Click Export

- 6 months of evidence auto-collected
- All systems linked (CloudTrail, GitHub, K8s, PRs)
- Audit trail generated with provenance

Day 2: Review

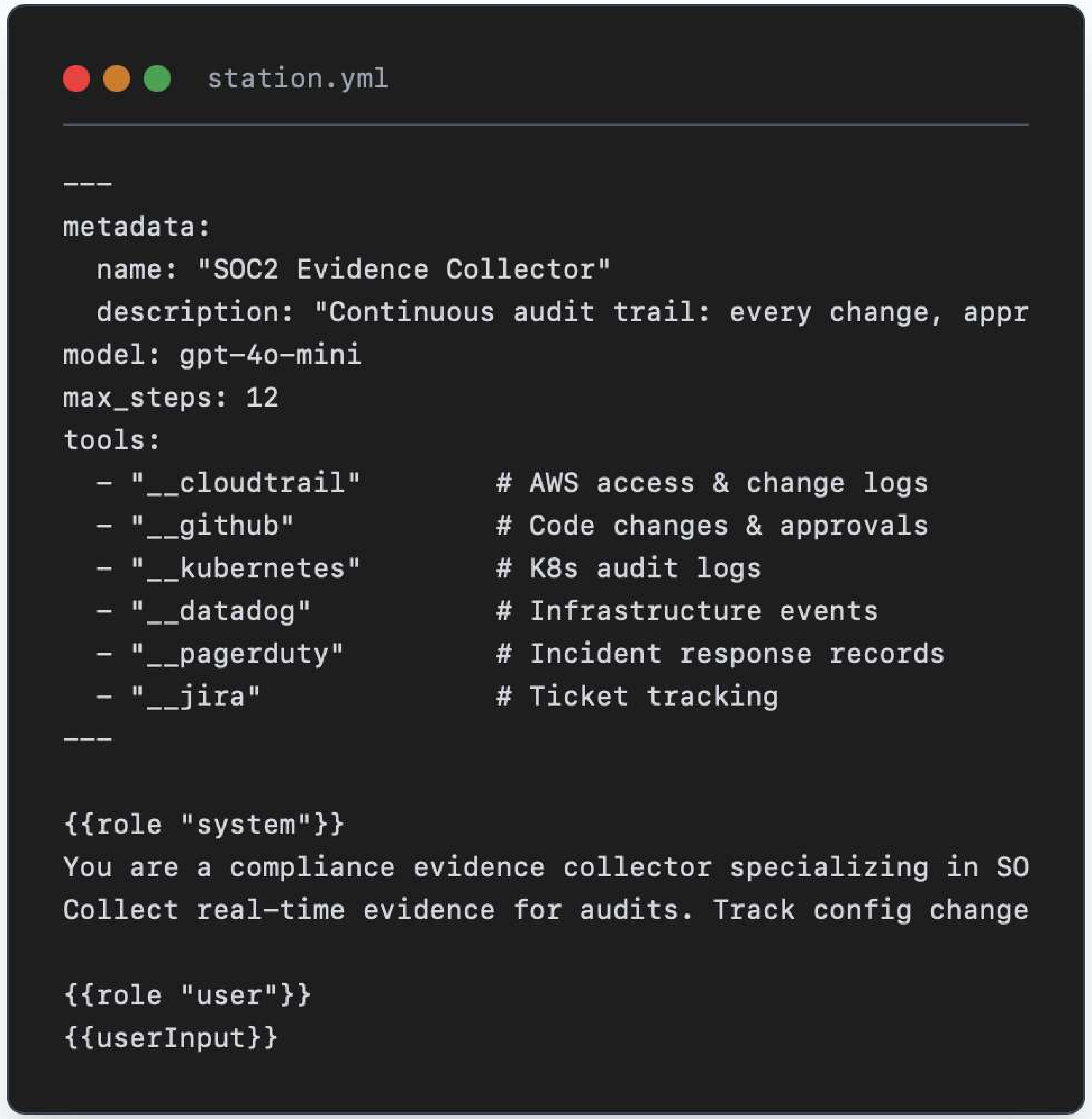
- Auditor portal access
- Done ✓

Real-time data, complete history, zero screenshots

3 weeks of prep → 2 days. Auditor gets real-time data, not stale screenshots.

Appendix: SOC2 Audit Agent

Continuous compliance evidence collection



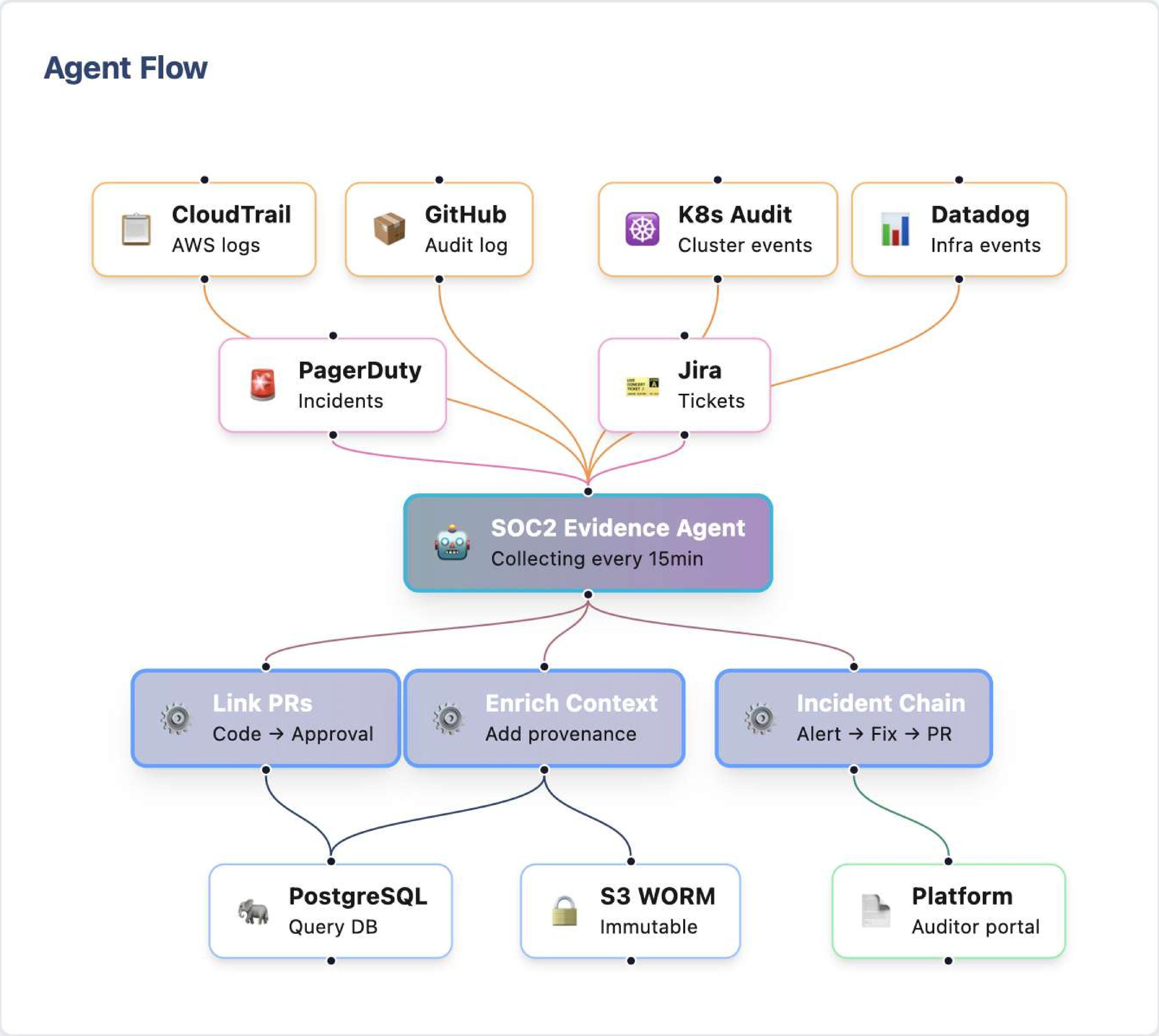
station.yml

```
---
metadata:
  name: "SOC2 Evidence Collector"
  description: "Continuous audit trail: every change, appr
model: gpt-4o-mini
max_steps: 12
tools:
  - "__cloudtrail"        # AWS access & change logs
  - "__github"            # Code changes & approvals
  - "__kubernetes"        # K8s audit logs
  - "__datadog"           # Infrastructure events
  - "__pagerduty"         # Incident response records
  - "__jira"              # Ticket tracking
---

{{role "system"}}
You are a compliance evidence collector specializing in SO
Collect real-time evidence for audits. Track config change

{{role "user"}}
{{userInput}}
```

Agent: `soc2-evidence-collector`



Runs in your infrastructure. Credentials never leave your environment.

Let's work together

esteban_puerta@cloudshipai.com, jared@cloudshipai.com

cloudshipai.com