



# Elvanto

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 A



# 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



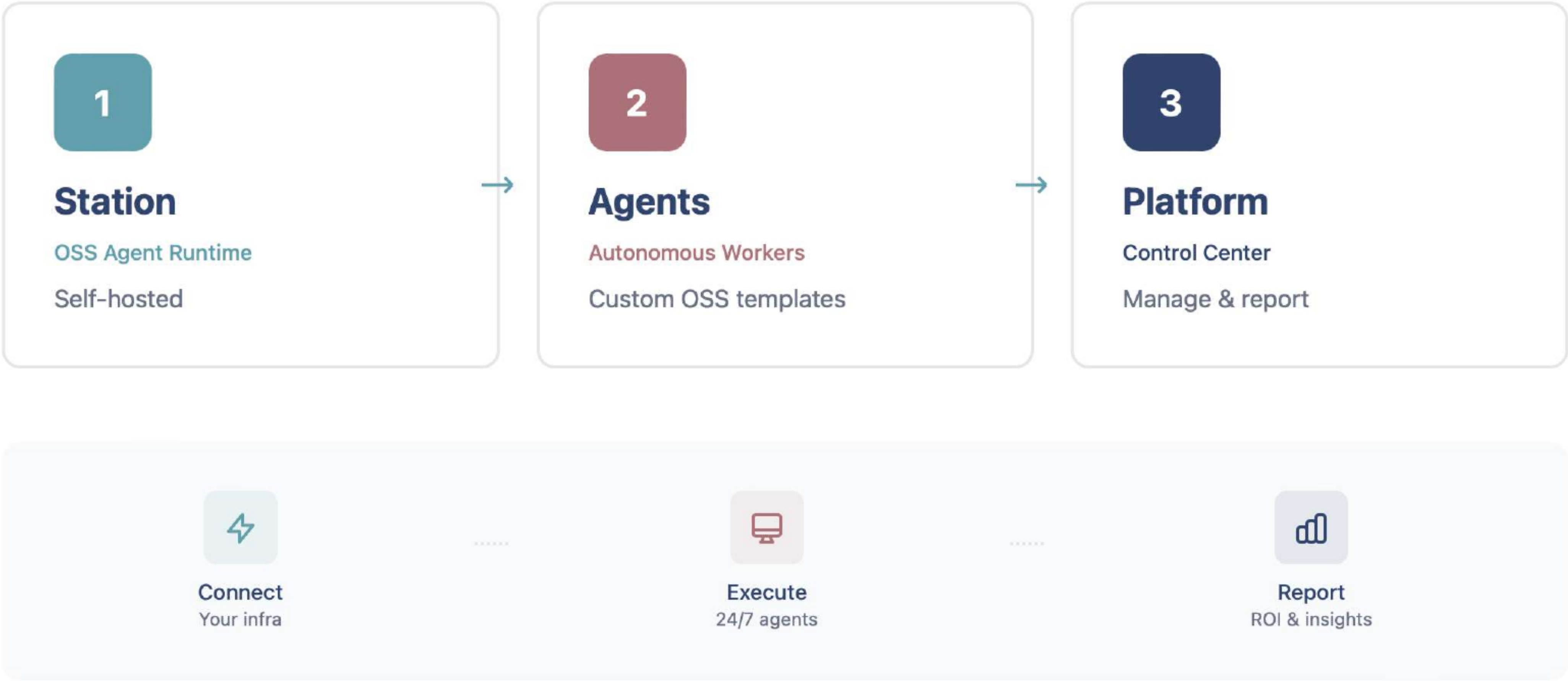
Every company becomes a tech company. Every team becomes agent-powered.

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 Elvanto Suite

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





# 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               | <del>Docker Swarm basic permissions</del> |
| GitLab          | Teams will not manage permissions across 8+ security tools          | Built-in security scanning      | <del>Tool sprawl</del>                    |
| HashiCorp Vault | Teams will not scatter AWS keys across config files and env vars    | Centralized secrets management  | <del>Scattered credential files</del>     |
| Elvanto         | Teams will not give credentials to cloud agents they do not control | Local-first OSS agent templates | <del>Cloud agents</del>                   |



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.

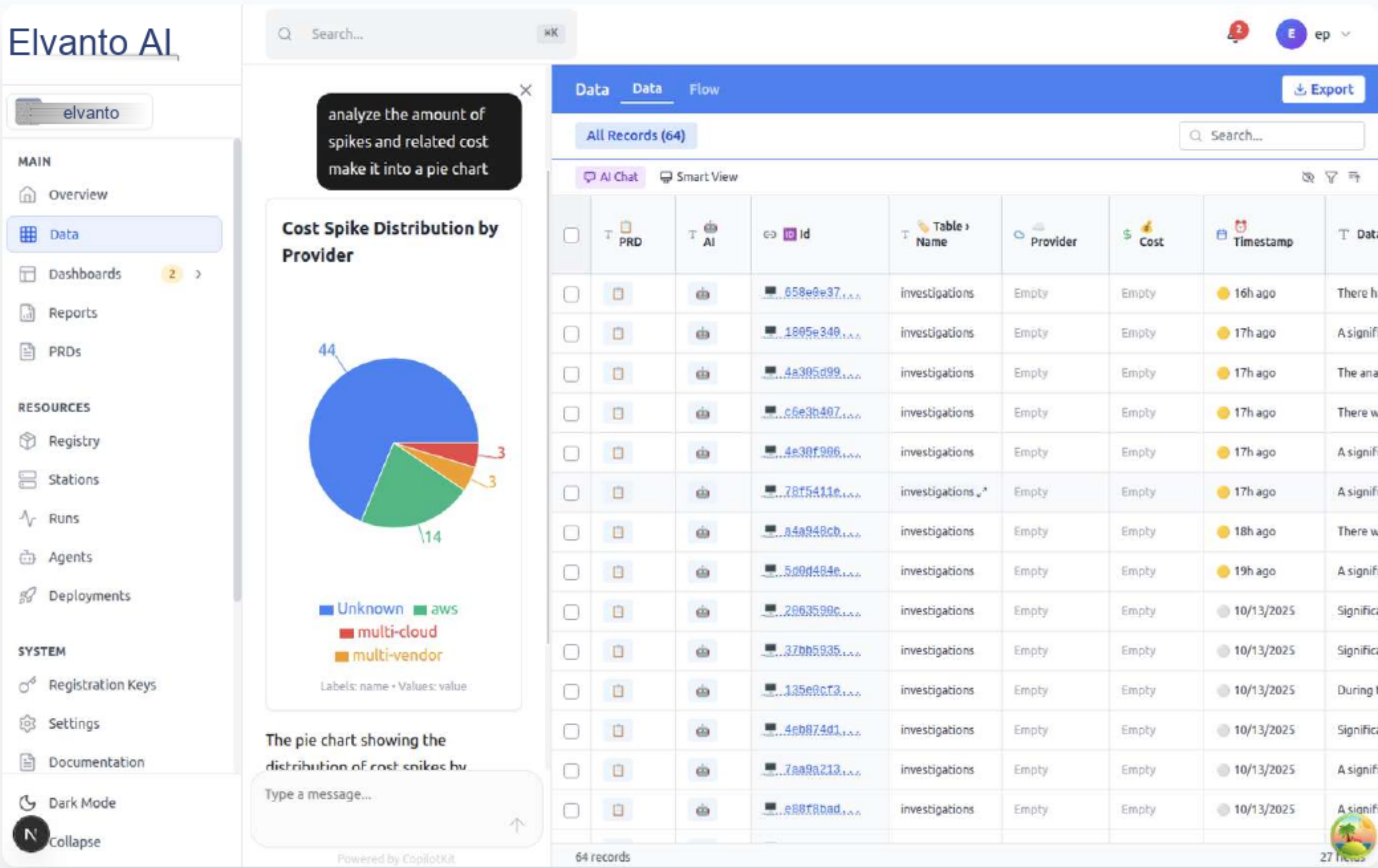


# The Elvanto Platform

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

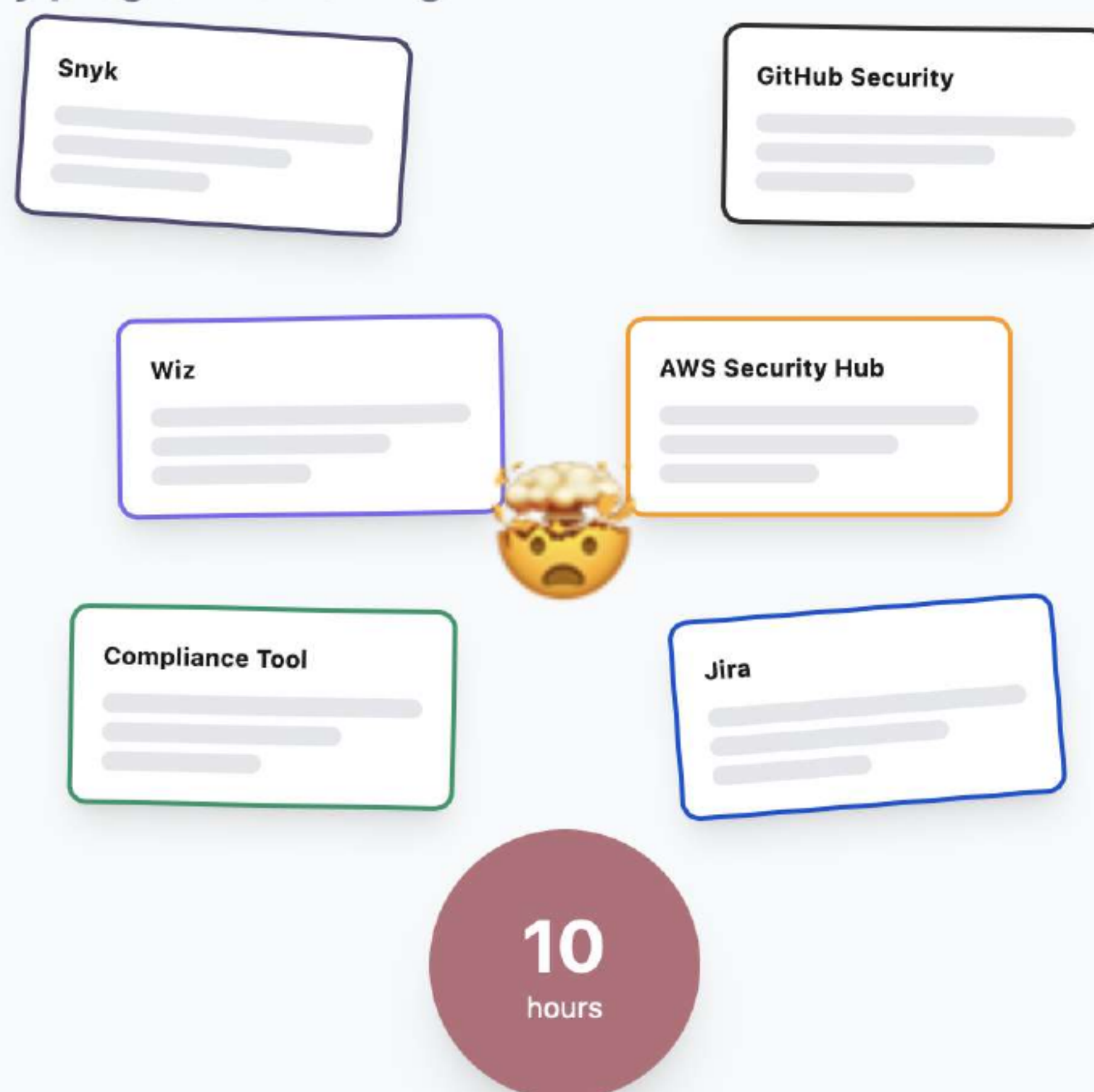
Each agent knows its job. Platform knows everything.





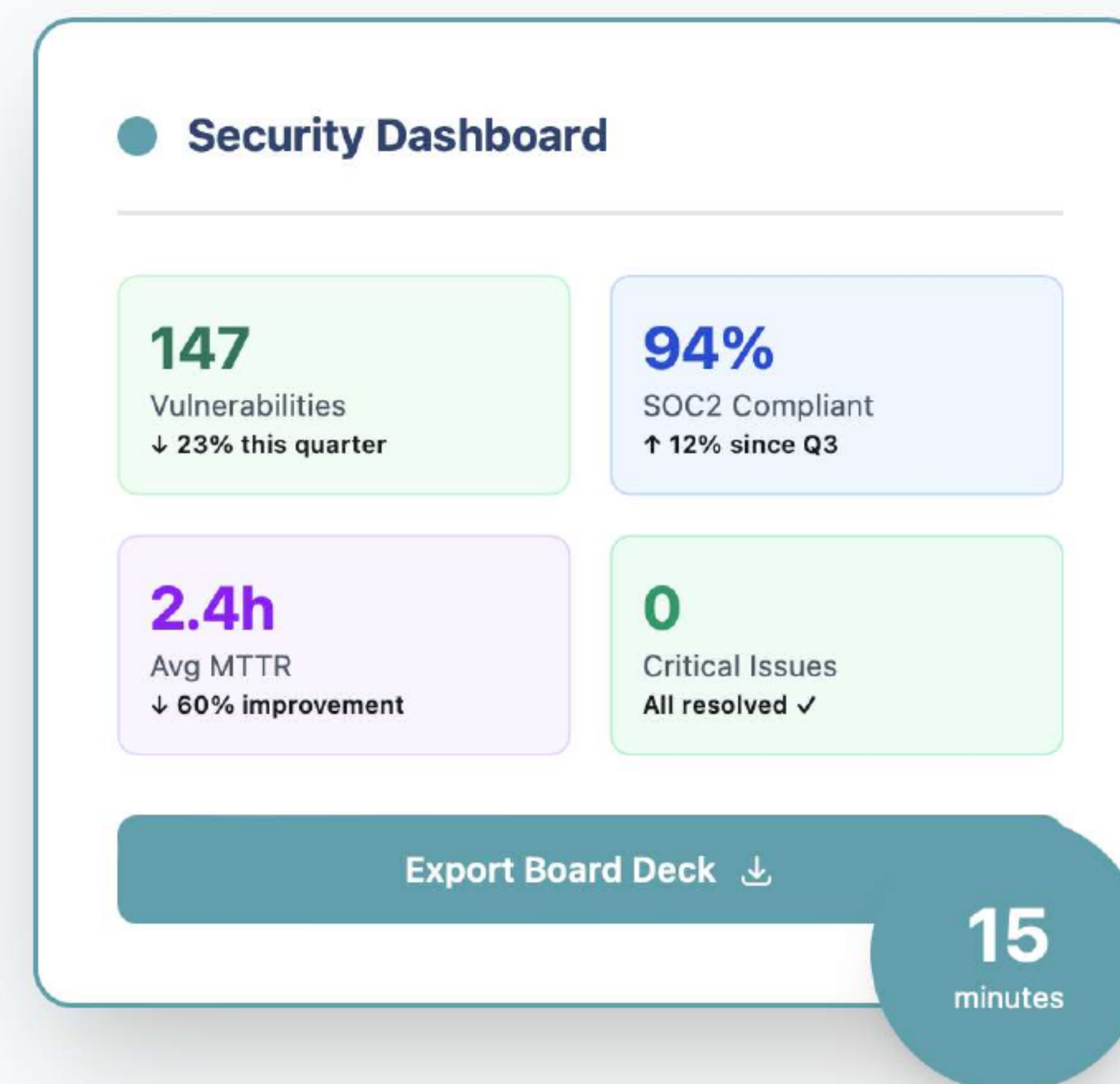
# Use Case: Security Metrics for the Board

Prove your security program is working



## Security Tool Sprawl

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



## 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

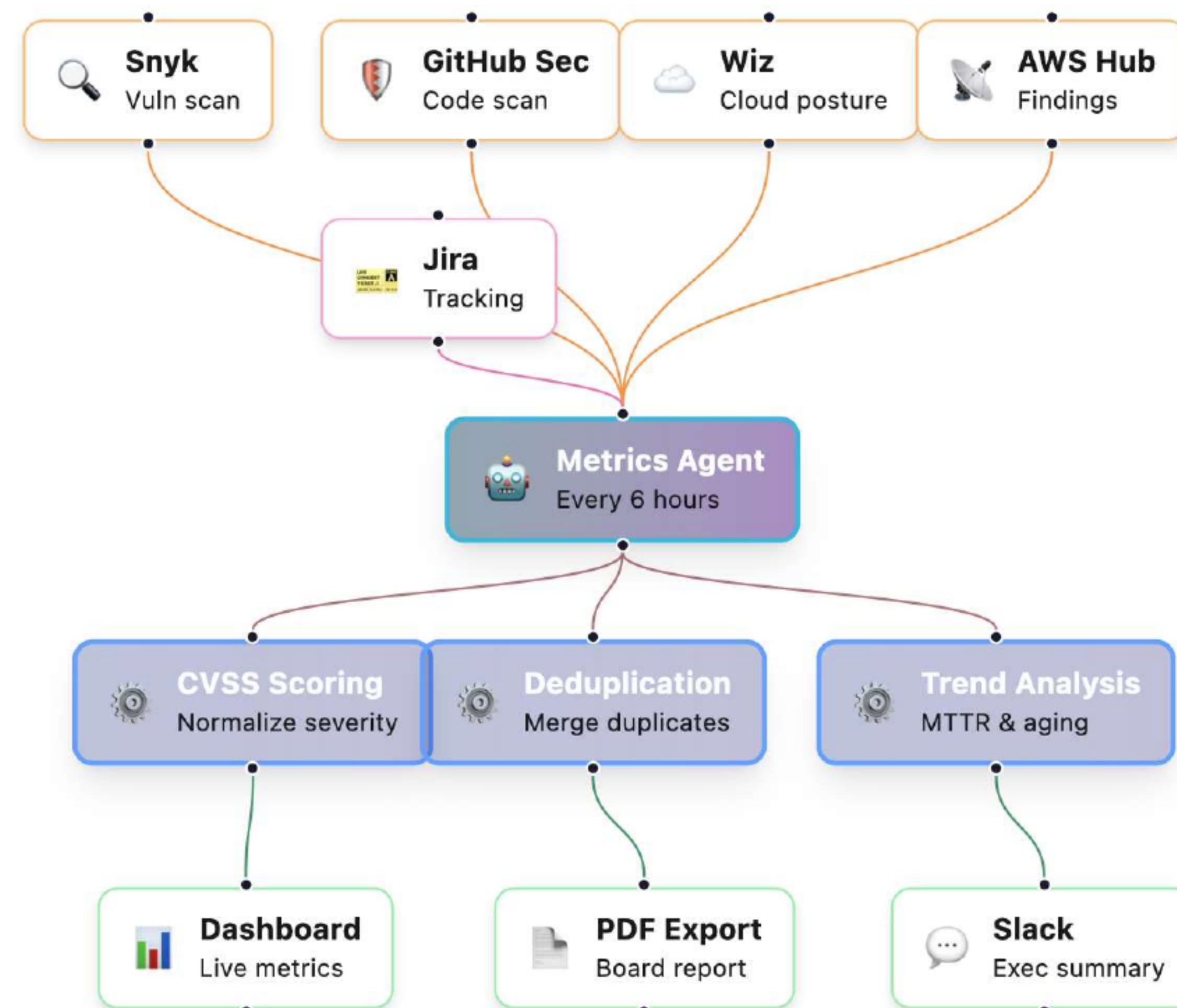
---
metadata:
  name: "Security Metrics Aggregator"
  description: "Unify 6 security tools → single board-read"
  model: gpt-4o-mini
  max_steps: 8
  tools:
    - "__snyk"          # Vuln scanning (750+ policies)
    - "__github_security" # Code scanning & Dependabot
    - "__wiz"           # Cloud security 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

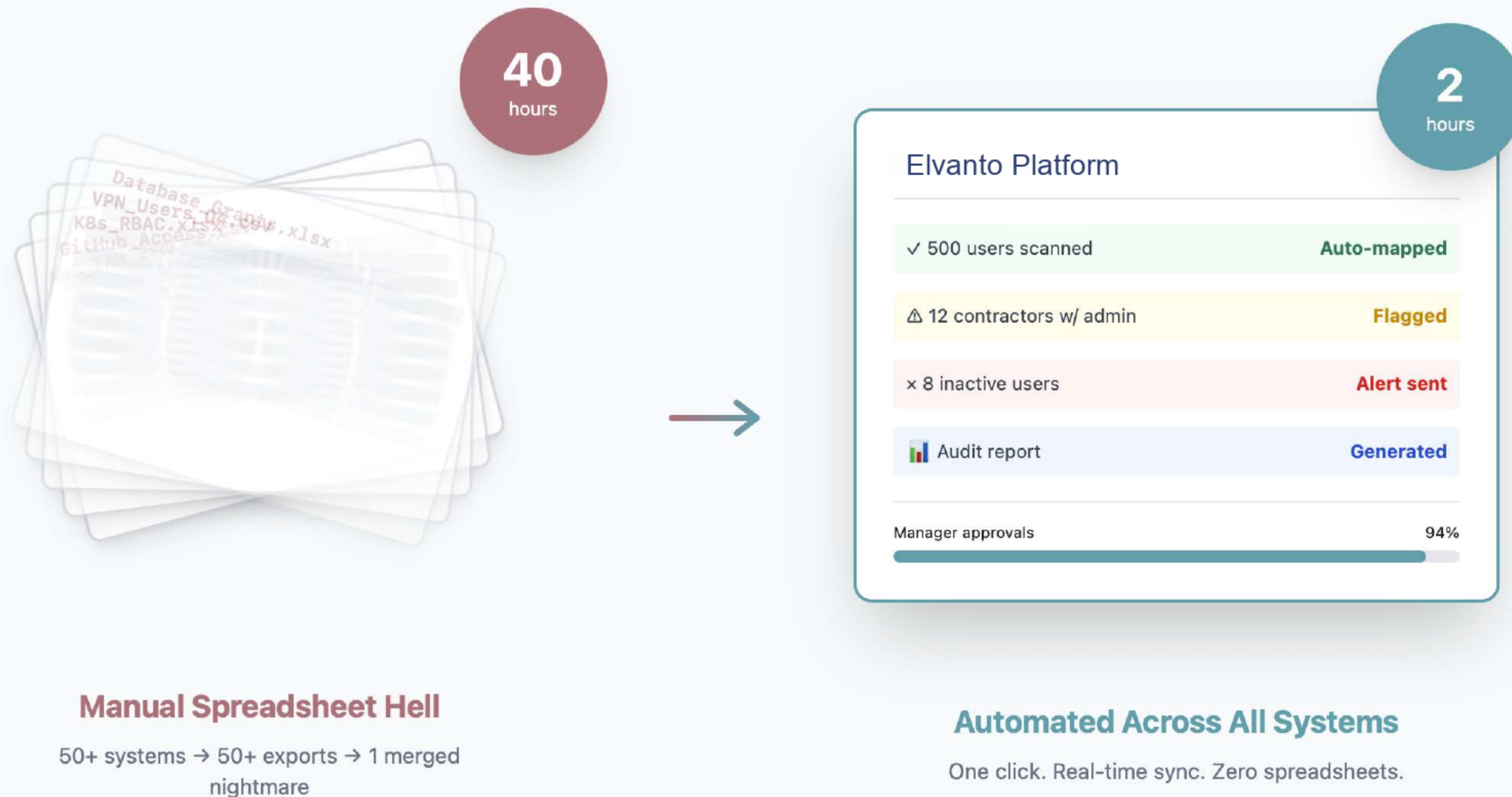
## Agent Flow





# Use Case: Quarterly Access Reviews

Required for SOC2, ISO27001, and PCI compliance



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



# Appendix: Access Review Agent

How it works under the hood

```
station.yml

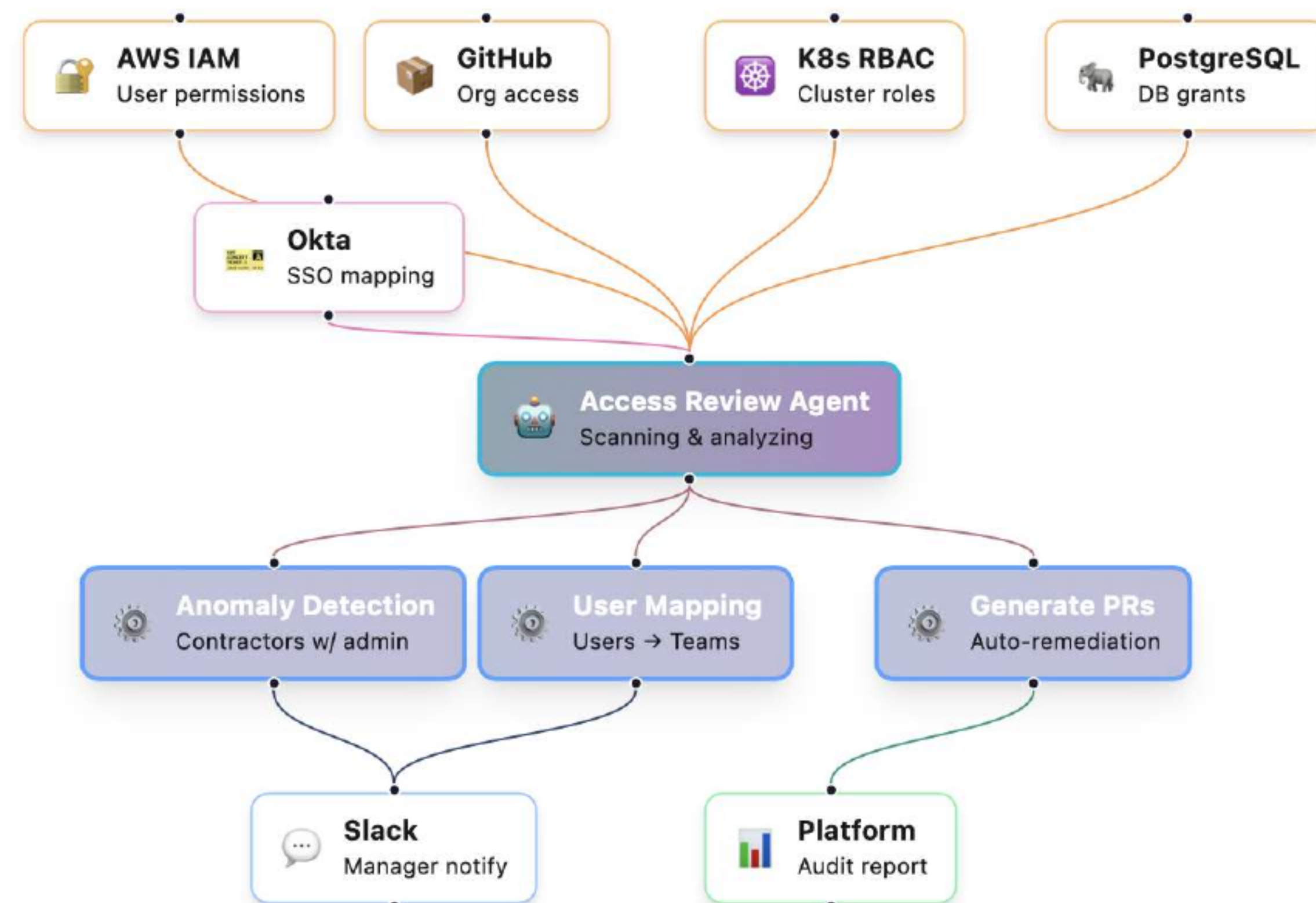
---
metadata:
  name: "Quarterly Access Review"
  description: "Scans 50+ systems, maps users to teams, fl
model: gpt-4o-mini
max_steps: 10
tools:
  - "__aws_iam"          # AWS IAM policies & users
  - "__github"           # GitHub org/team permissions
  - "__kubernetes"       # K8s RBAC roles & bindings
  - "__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



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 Elvanto: 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

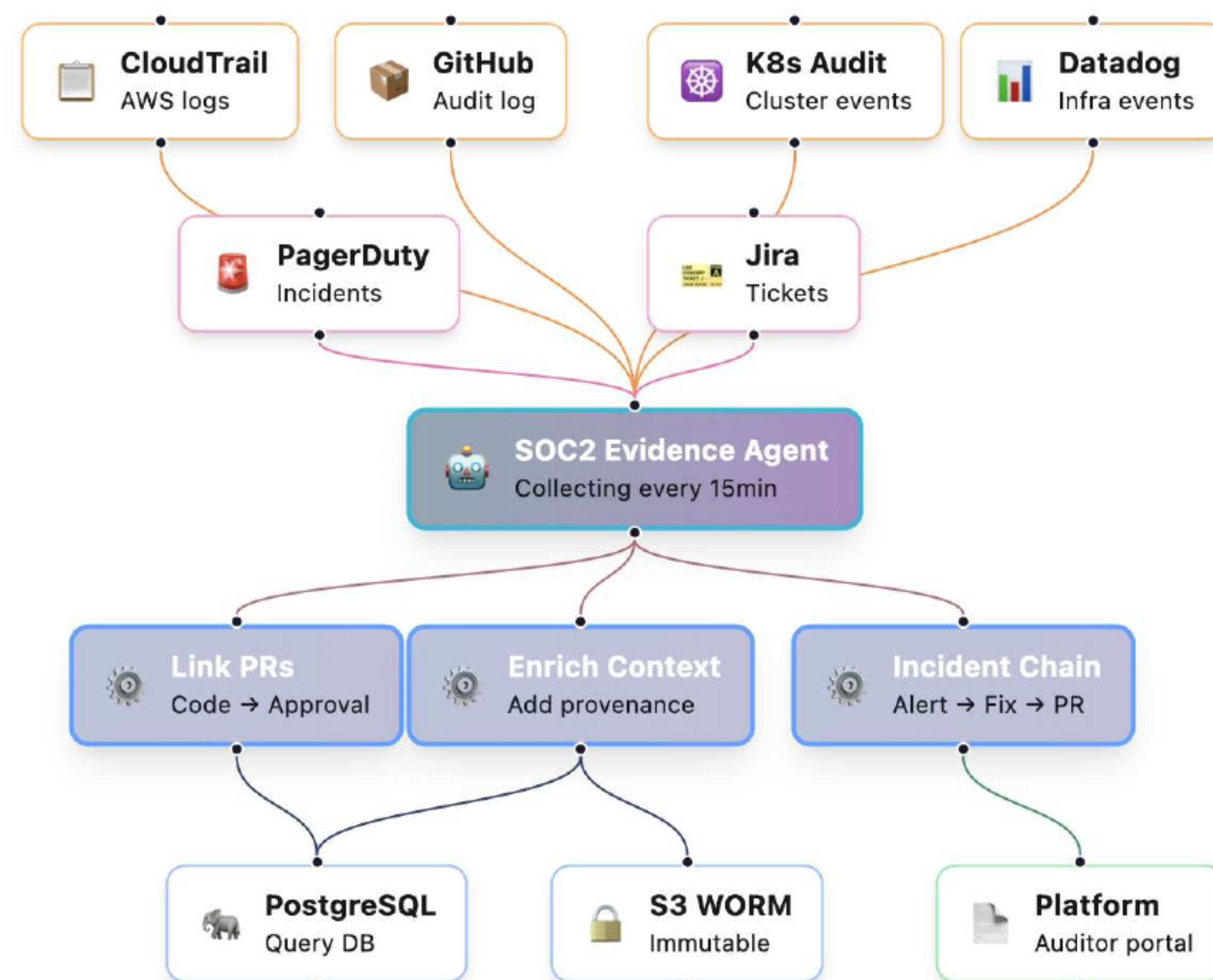
---
metadata:
  name: "SOC2 Evidence Collector"
  description: "Continuous audit trail: every change, appr
model: gpt-4o-mini
max_steps: 12
tools:
  - "__cloudtrail"      # AWS access & change logs
  - "__github"          # Code changes & approvals
  - "__kubernetes"      # K8s audit logs
  - "__datadog"          # 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

## Agent Flow







# Let's work together

legal@elvanto.app

elvanto.app