

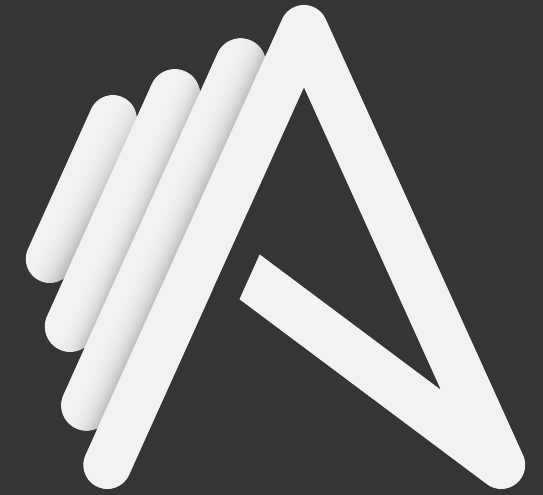
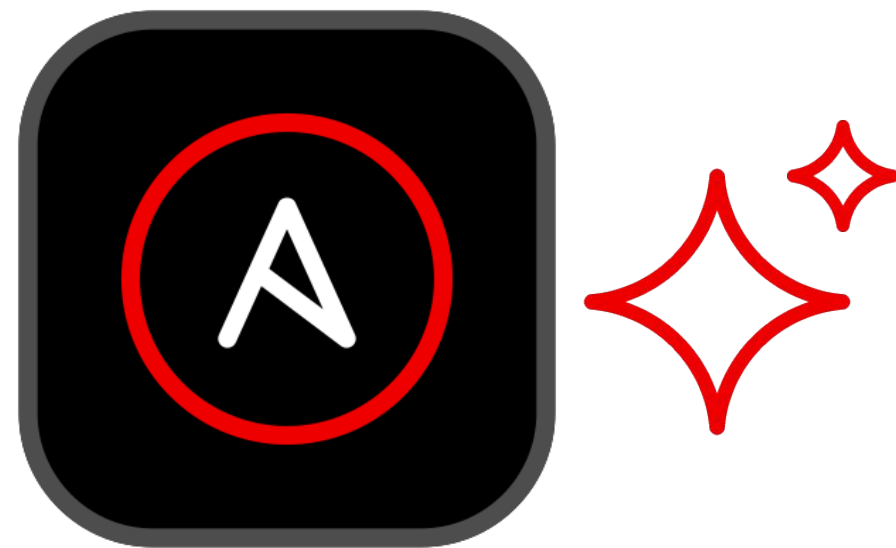
(Sovereign) AIOps

Red Hat Ansible + AI for IT Infrastructure



What is AIOps?

Understanding Ansible for AI assisted operations



What do we mean by “AIOps”?

AIOps | Turn operational insight into intelligent, automated outcomes.

Ansible Automation Platform is the ***trusted execution and orchestration*** layer for AIOps, integrating AI and partner intelligence into governed, reusable automation at scale.

And how is sovereign related?

Sovereign | Keep total control of
your technical stack and data.

You can choose if you give control of technical stack and access to data in your own hands or do trust it to third parties.

Why do we do this?

We want to achieve

- Speed to resolution and root cause analyzes
- Avoid spending time on what is quickly done by AI
- Yet, we want process that is:
 - Auditable
 - Repeatable
 - Versionable
 - Predictable

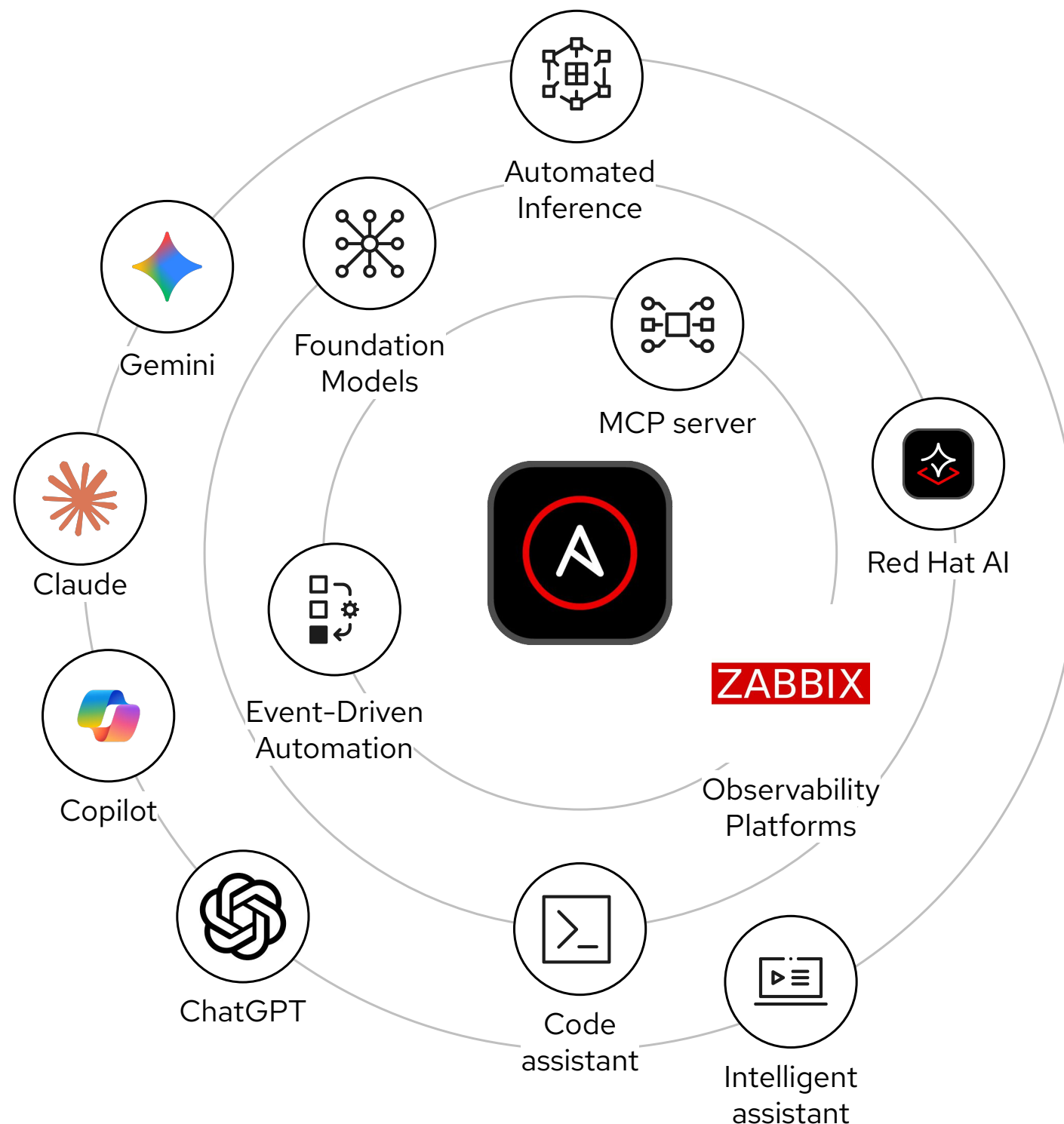


AIOps with Ansible Automation Platform

AI-powered operational framework for IT infrastructure

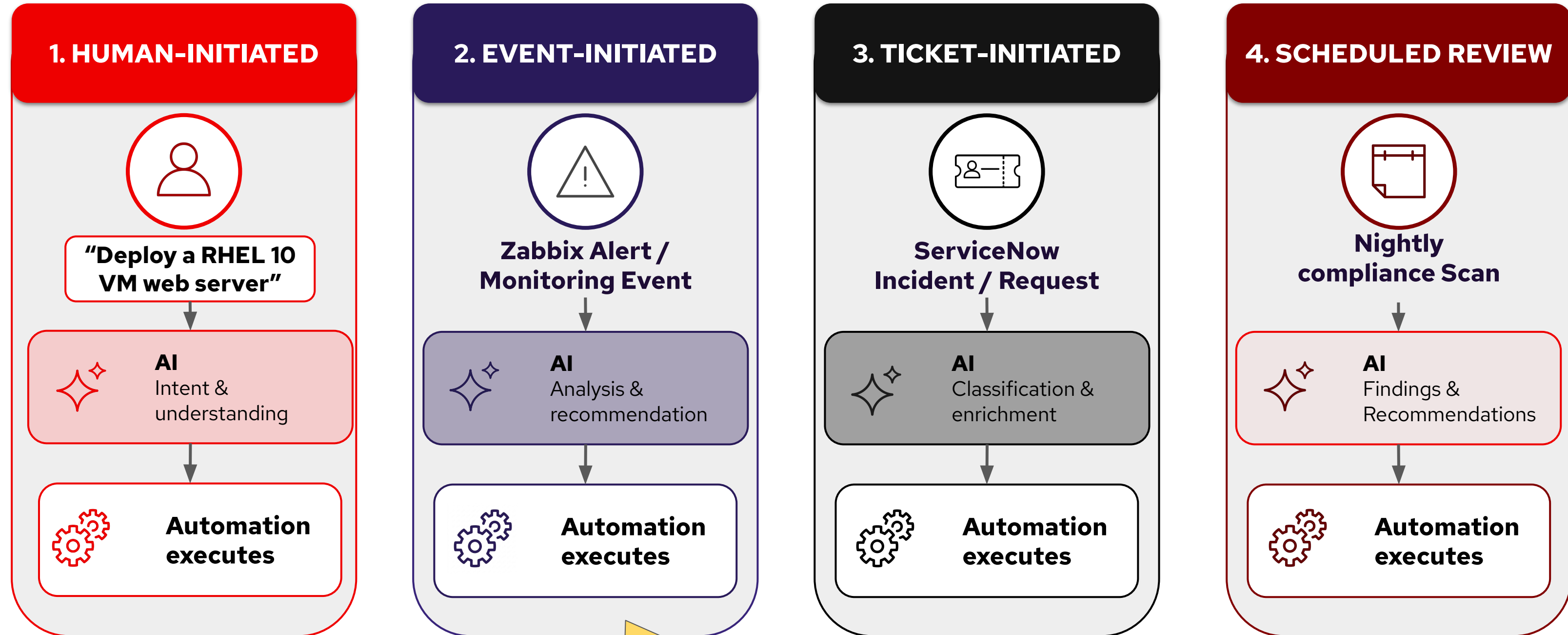
- > Ingest telemetry, alerts, and operational events from observability and IT platforms
- > Use AI to enrich incidents with context and recommended remediation
- > Automate corrective actions through trusted automation workflows
- > Enable human-in-the-loop approvals for governed operations

Turn operational insights into automated action across your infrastructure



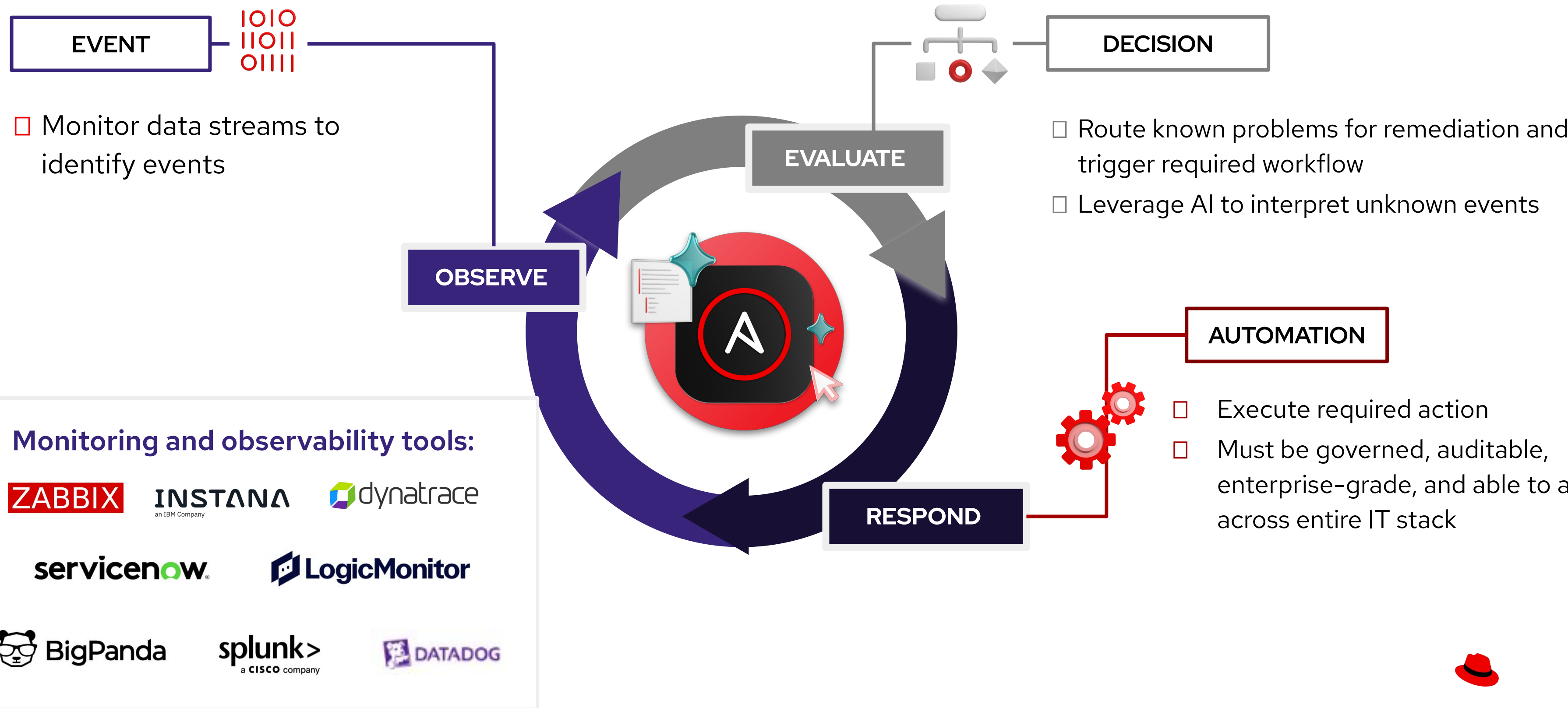
Where does AI participate?

AI Ops is not defined by how work starts

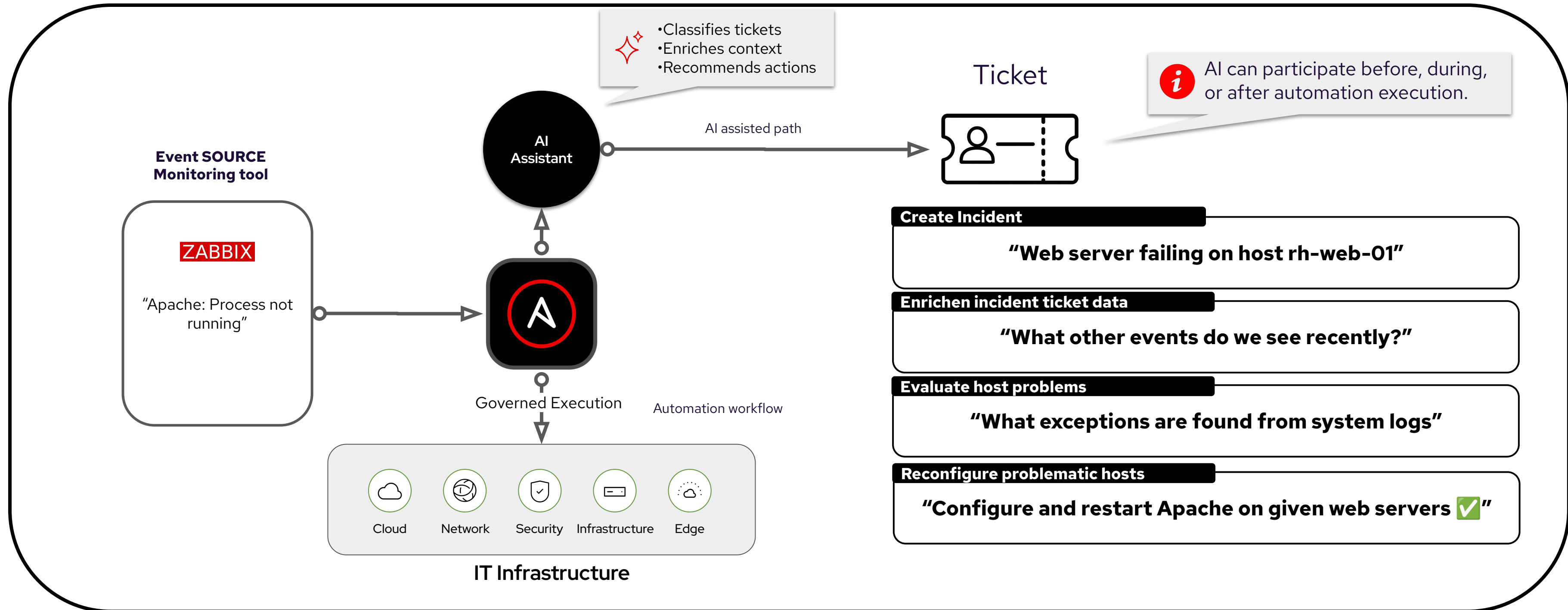


Today's we focus on event-driven

2. AI-Assisted Event Response



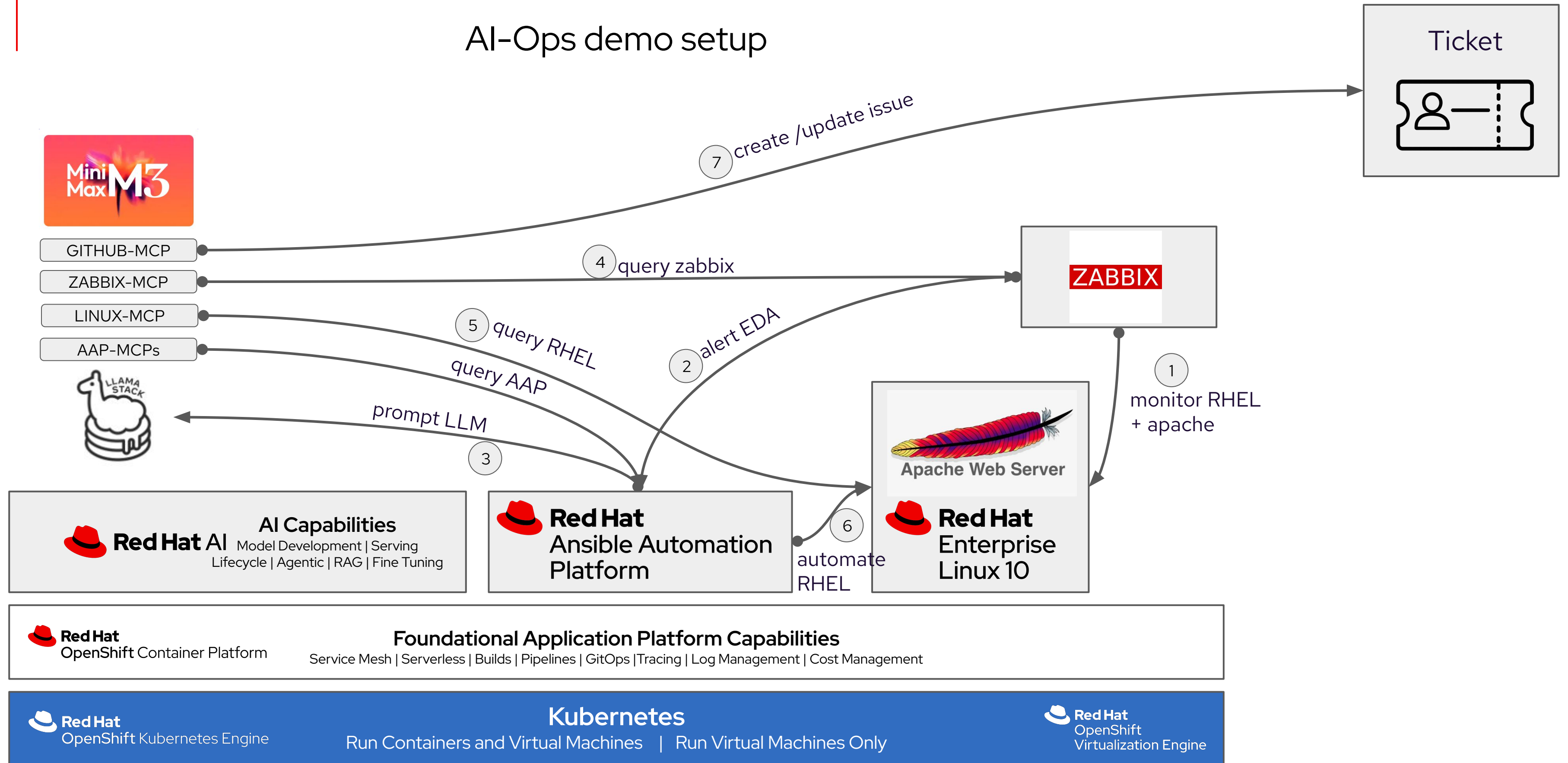
3. AI-Enriched Ticket Resolution



Takeaways:

- AI accelerates triage and decision making and helps avoiding future problems by pointing root cause.
- Ansible Automation Platform provides orchestration, governance, and auditability to execute across any environment and any tool.

AI-Ops demo setup

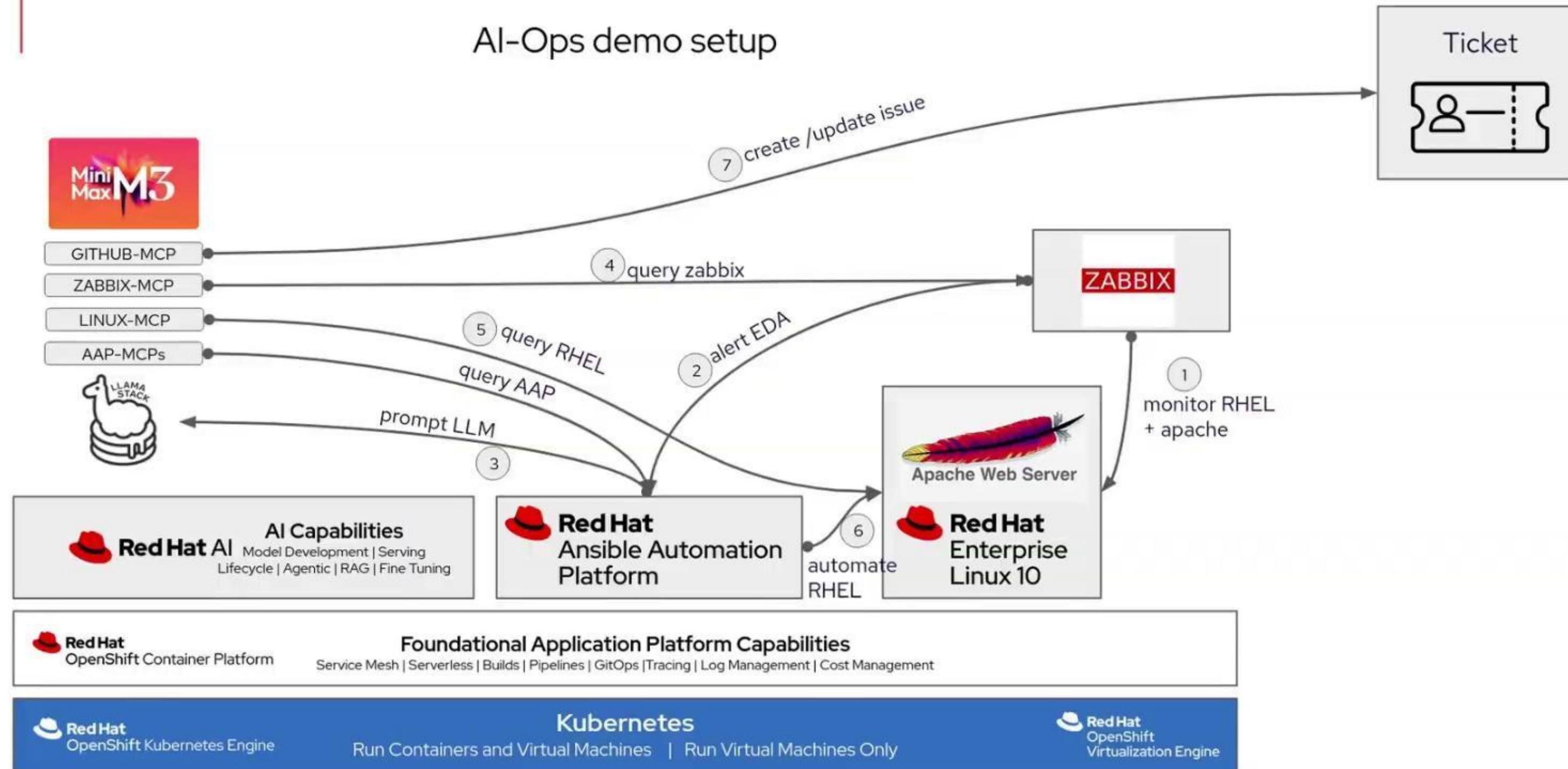




DEMO TIME



AI-Ops demo setup



Going further...

- ▶ Use professionals for Zabbix, this was just a simplest demo 😊
- ▶ Combine info about Red Hat insights reports 📋
- ▶ Pull info from Satellite about compliance to CIS/NIST/etc... governance tooling ✅
- ▶ In container and virtualization world, utilize ArgoCD / OpenShift GitOps 
- ▶ There are MCPs for all kinds of a systems, networking, storage etc.. to pull information from / Push configurations to using ansible collections

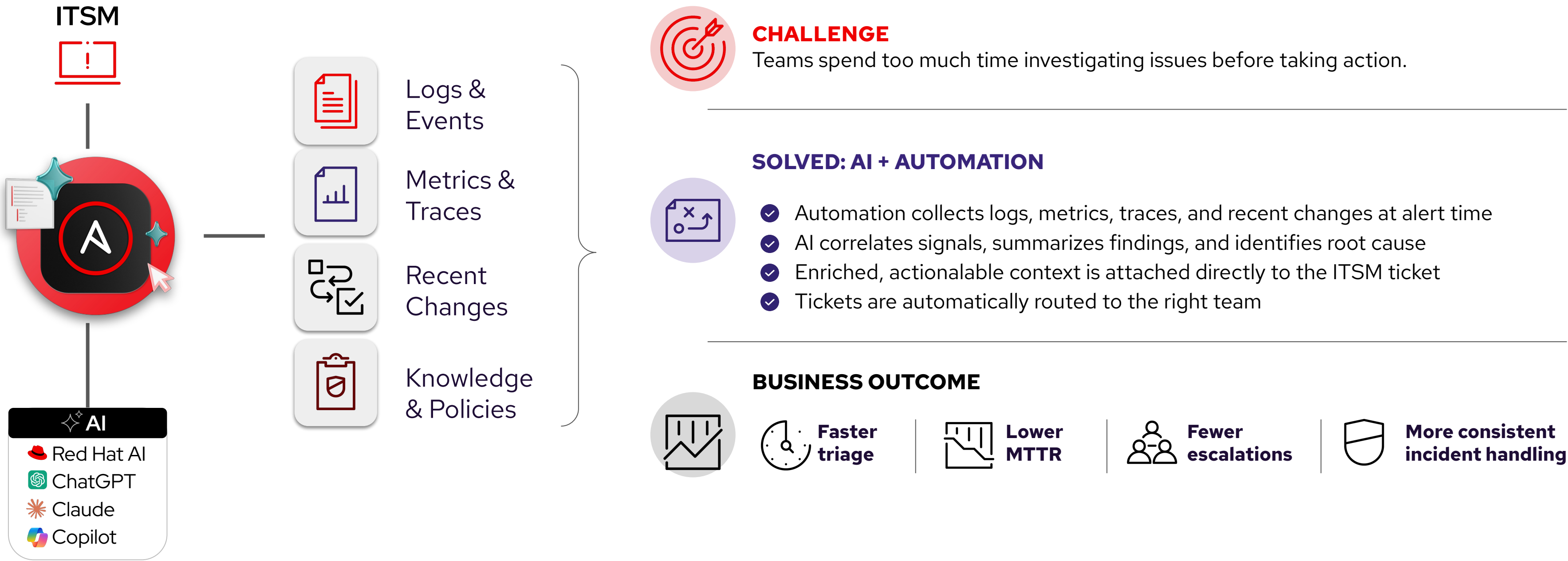
Should we harden this somehow?

Sure, this is just a demo cutting all the corners...

- ▶ Do we need MCP gateway for authentication?
- ▶ Is RBAC set properly in AAP/git so that prompts can't be manipulated?
- ▶ Can the data be poisoned? E.g. something breaking the prompts in server logs?
- ▶ Strong guardrailing of the models and MCPs so that they can only read?

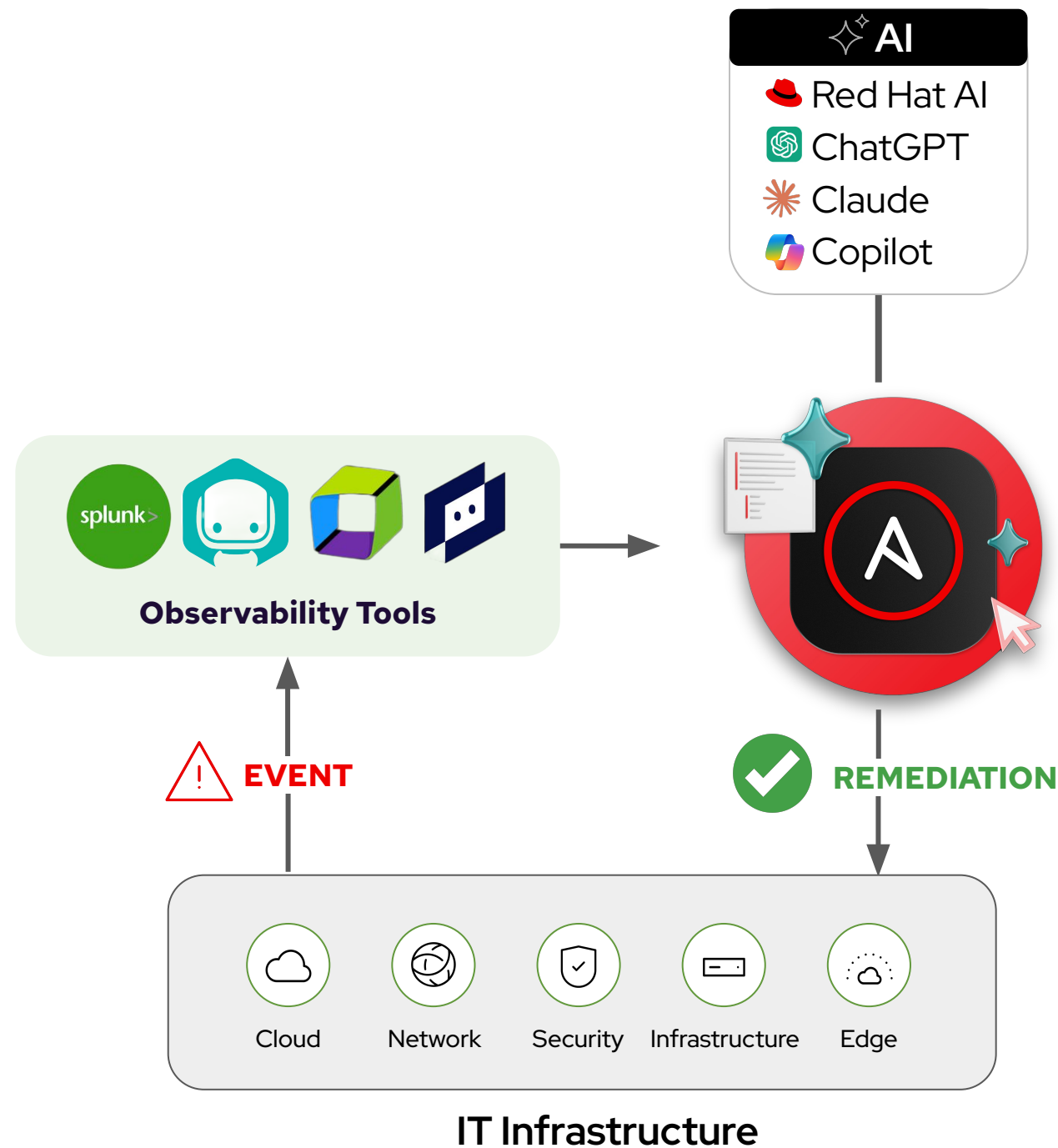
Incident and ticket enrichment

Accelerating diagnosis by attaching context at the moment an incident is created



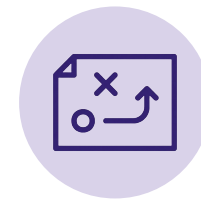
Self-healing infrastructure

Observability, AI, and automation are combined into a closed-loop operational system



CHALLENGE

Known issues with proven fixes still wait in alert queues for someone to pick them up, diagnose them, and run the remediation manually causing delay, inconsistency, and interruption.



SOLVED: AI + AUTOMATION

- ✓ Observability platforms detect systems-level failures using continuous signals
- ✓ AI interprets the signal and generates or adapts remediation
- ✓ Automation executes remediation using approved workflows and permissions



BUSINESS OUTCOME

- Faster Recovery**
- Consistent operations**
- Scalable adaptability**
- Controlled autonomy**



The Bottom Line: Self-healing infrastructure closes the loop between detection, remediation, and validation

Thank you



linkedin.com/company/red-hat



youtube.com/AnsibleAutomation



facebook.com/redhatinc



x.com/Ansible



Red Hat Ansible Automation Platform