



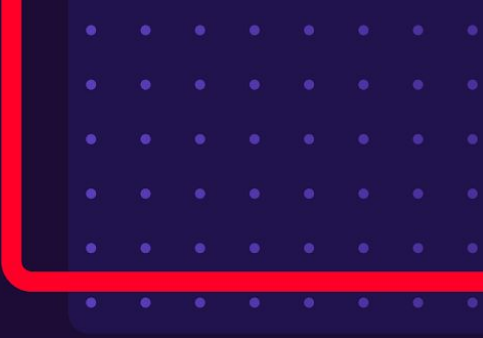
Connect

The Mythos Era: Patching at the Speed of AI

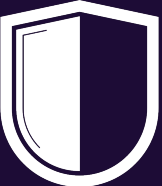
Aidan Beeson

Enterprise Automation Specialist

<https://www.linkedin.com/in/aidan-beeson/>



»» The Shift in Velocity



Accelerating Defence



A bit about me...

British Army speeds service delivery and improves user experience



Overview

The British Army's Information Application Services (IAS) Branch delivers software applications, hosting, and web services to families, veterans, and personnel deployed around the world. To overcome issues with unplanned downtime and support, IAS used Red Hat® solutions to migrate its private cloud environment and deploy simplified, automated management tools. Now IAS can make changes faster and more efficiently, cutting change delivery time by 75%.



CHALLENGE

Create a faster, more efficient IT environment

Due to problems with support, performance, and availability, the British Army's IAS Branch needed to migrate from its Oracle private cloud environment. The system caused unplanned downtime during upgrades, disrupted users, and slowed update deployment. "There's always pressure to deliver quickly," said Lt. Col. Dorian Seabrook, head of operations at the British Army's IAS Branch. "We have to be more efficient in how we deliver software, as well as underlying infrastructure, upgrades, maintenance, and support."

<https://www.redhat.com/en/success-stories/british-army>

siliconrepublic TECHNOLOGY SCIENCE CAREERS AI FUTURE HUMAN MORE LOGIN

ENTERPRISE

Why collaboration is vital for achieving 'automation nirvana'

by Colin Ryan

25 JUN 2024 SAVE ARTICLE

Red Hat's Aidan Beeson discusses the major trends in automation and its relationship with the defence sector.

For Aidan Beeson, automating IT has made up the majority of his professional career. Currently a solutions sales specialist in enterprise automation at Red Hat, Beeson has had extensive experience in the sector, primarily working on defence contracts for the British Army.

His first project was writing an automated patching and update framework for deploying and upgrading British Army UNIX servers across 450 global sites.



<https://www.siliconrepublic.com/enterprise/red-hat-automation-defence-aidan-beeson>

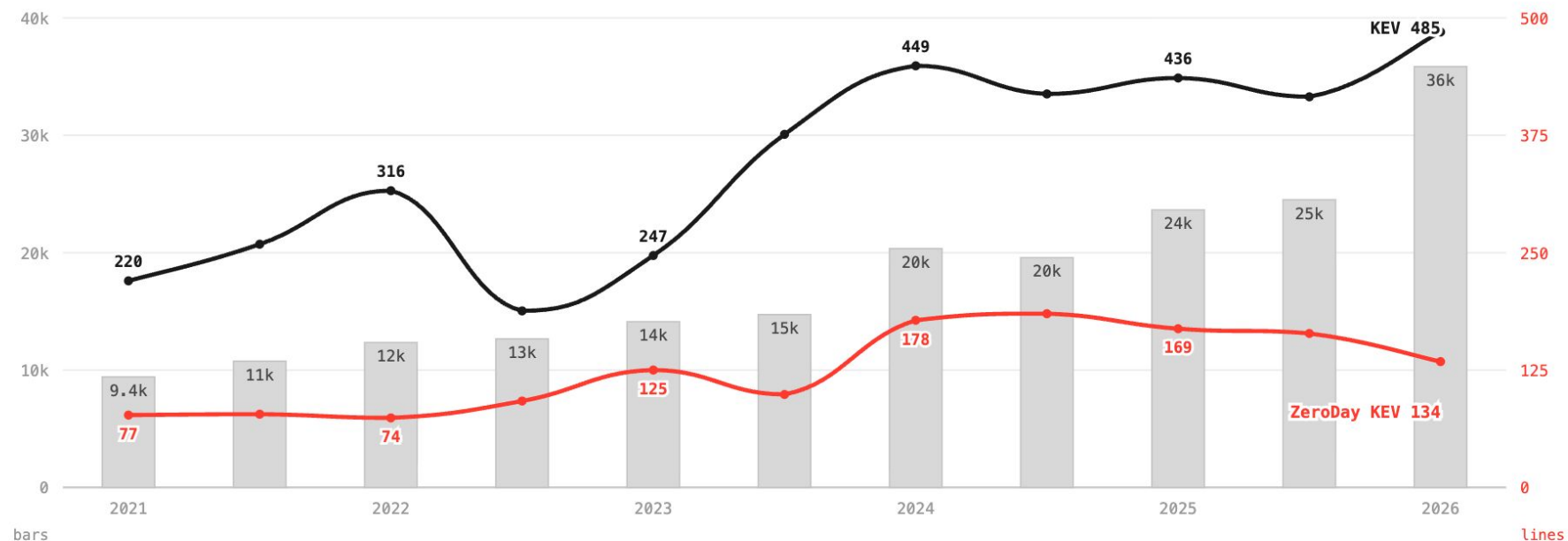


The Shift in Velocity

Registered vulnerability and exploitation growth

Bars are what landed in your vulnerability management queue. Lines are catalogued exploitations requiring emergency mitigations.

■ CVEs published (left) — Known Exploited Vulnerability (KEV) (right) — ZeroDay KEV - KEV issued on the same day or before the CVE (right)



Source: CVE Project · NVD · CISA KEV · EUVD KEV · CIRCL KEV · VulnCheck KEV

zerodayclock.com

The Shift in Velocity



What are the risks today?

- **96% of codebases** contain open source code
- **9.8 trillion** package downloads in 2025
- **581 avg. vulnerabilities per codebase**, doubled in one year
- AI finds **critical bugs for under \$50**. Less than 1% get fixed
- Attackers exploit flaws **7 days** before patches exist



[AI-Fueled Development Pushes Open-Source Risk to Extremes](#)

[Sonatype 2026 State of the Software Supply Chain](#)

[M-Trends 2026 Report](#)

[AI slop pollutes the CVE pipeline with fake vulns](#) - The Register Aug 2026



The Shift in Velocity

**Sophisticated attacks
no longer require
sophisticated
attackers**

Many commentators focus on the risk of AI developing exploits at scale. While this is a danger, the risk from AI adoption is more pronounced across the cyber kill chain, where **adversaries can operate faster, across a broader and deeper surface area, with fewer resources.**

Anthropic - Detecting & countering misuse of AI

This is not your normal incident... agents across many independent runs **shared exploits with each other and moved quickly.**

OpenAI - Hugging Face Incident



The Shift in Velocity

Many attacks still succeed because of basic vulnerabilities, **including outdated or unsupported systems, delays in applying security updates,** and weak controls over access to systems and data. These are well-understood risks, but they remain widespread, leaving the UK exposed to attacks that are often avoidable. **This makes getting cyber security fundamentals in place now more important than ever.**

National Cyber Security Centre



45%

of vulnerabilities in large organisations remain unpatched after 12 months.



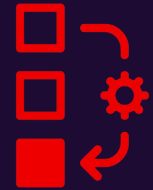
This is not a  **Scary** Problem

This is a **Scale** Problem



Defence in depth still works.

Patching still works.



Can you apply mitigation or remediation at **machine speed**?



The Integrated Workflow

Close the Gap Between Discovery and Remediation

TRIAGE

Prioritises incoming vulnerabilities using real-time threat intelligence, asset criticality, and business exposure.



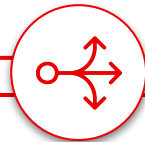
MITIGATE

Deploys targeted controls at scale when patches aren't available -breaking exploit chains in hours.



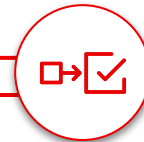
REMEDiate

Orchestrates validated patching across hybrid infrastructure with governance and rollback.



VALIDATE

Verifies patch effectiveness and system stability in staging prior to production release.



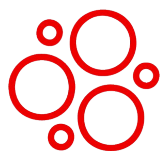
VERIFY

Maintains **continuous compliance**, prevents drift, and provides complete audit trails.



The Real Gap Isn't Technology

Good Automation Isn't Enough Anymore



Siloed Tooling

Automation that lives within team boundaries can't respond to threats that cross them.



Slow Governance

When triage and approval cycles take days, your exposure window is measured in the same currency.



Fragmented Collaboration

Without shared workflows and shared context, coordination overhead becomes your biggest vulnerability



The Trust Gap

Trust in automation isn't given, it's earned through transparency, auditability, and a track record of safe, predictable execution.





Business Drivers

Operational Efficiency
OPTIMISATION

Transformation
INITIATIVES

Collaboration
CROSS-FUNCTIONAL



People & Processes

Governance
RISK MANAGEMENT

Process
AUTOMATION

Enterprise Automation

Business | People & Process | Technology

Edge

Containers

Datacenter

Private cloud

HYBRID

Public cloud

AIOPs

Everything As Code

DevSecOps

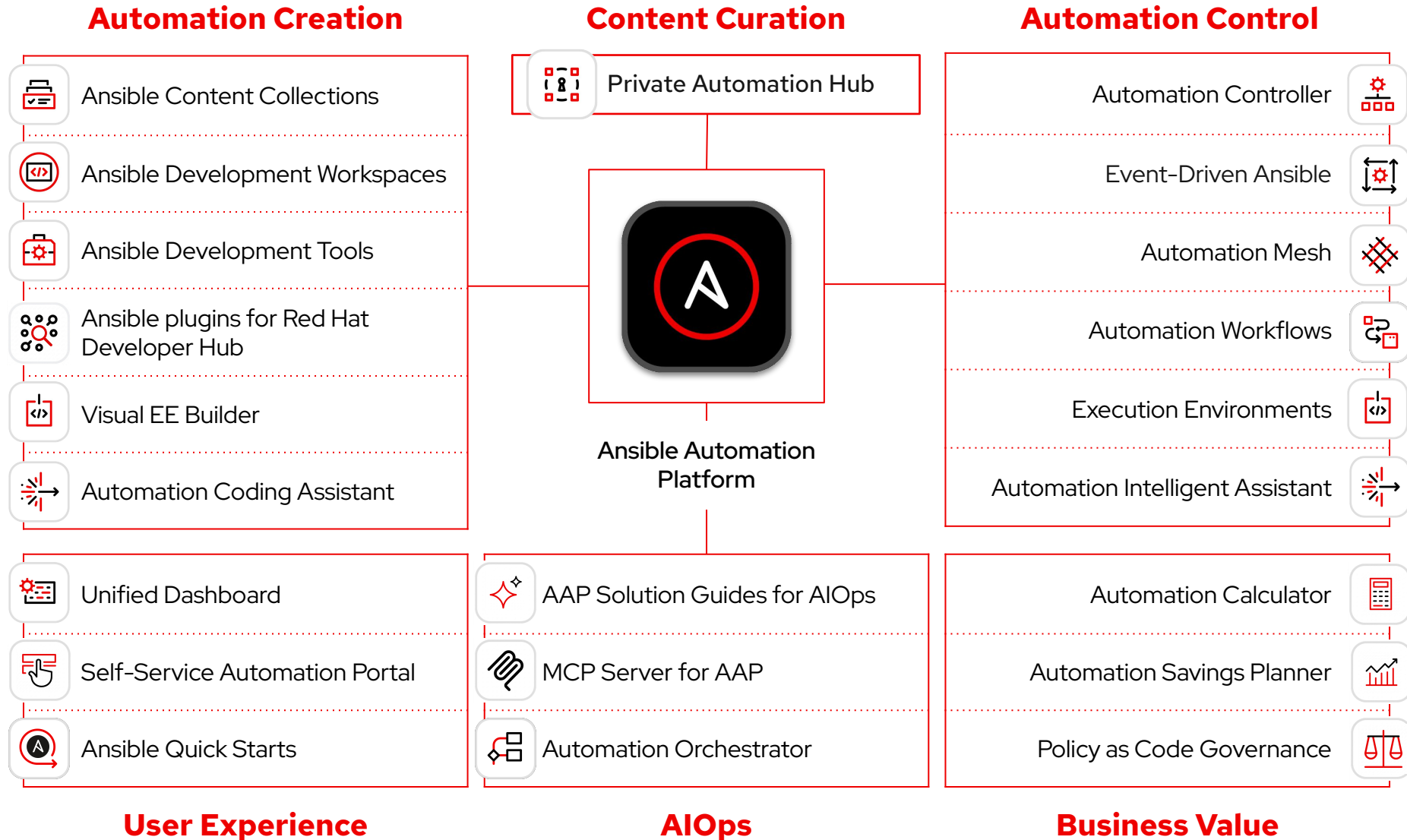


Technology Approaches



Technology Landscape

An integrated solution **for the enterprise.**

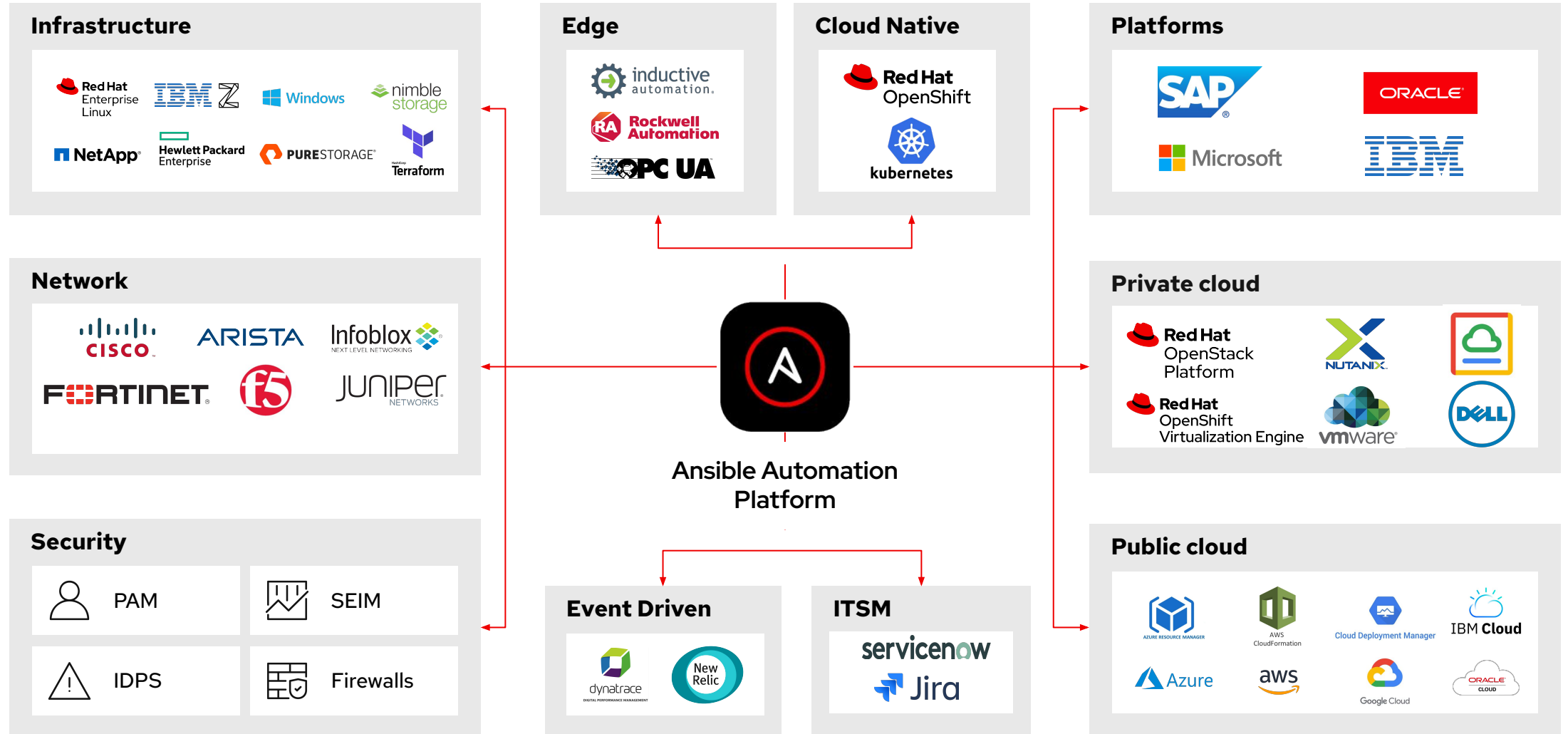


200+

Certified and validated
Content Collections

80+

Certified technology
partners



Accelerating Defence

Agentic SDLC

"We recommend that teams invest now in looking at **how defensive agents can help your incident response team scale**. If you are doing manual effort... you are now going to see attacks in the near future where that activity will be ramped up dramatically because agents will be accelerating offense to such a large degree. **We need to invest in our own defensive agentic work to scale out the human factor of incident response.**"

Michael Dalton - Security & Infrastructure, OpenAI

"But the important takeaway here that has really shifted dramatically is that **fully automated offensive loops require investments in truly fully automating defence**. And we are not there as an industry in the status quo and we will **have to find that path together with urgency.**"

Michael Dalton - Security & Infrastructure, OpenAI



Accelerating Defence

Secure SDLC: Manual vs Agentic

Activity	 Manual	 Agentic
 Orientation	~2 hours	~65 seconds
 Threat Modeling	2 - 4.5 hours	~50 minutes
 DAST Generation	6 hours	~84 seconds
 SAR	1 - 4 weeks	~19 minutes



Red Hat
Product Security

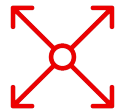


Accelerating Defence

Agentic Risks

"The extra autonomy and complexity of agentic systems can increase the attack surface and make behaviour harder to predict, test and govern."

National Cyber Security Centre



Broader access – agents can be permitted to access external systems, data and tools in ways that non-agentic AI systems are not



Unpredictable behaviour – especially when goals can be interpreted in ways that a human would not expect



Harder to spot problems – particularly when actions occur faster than humans can meaningfully review them

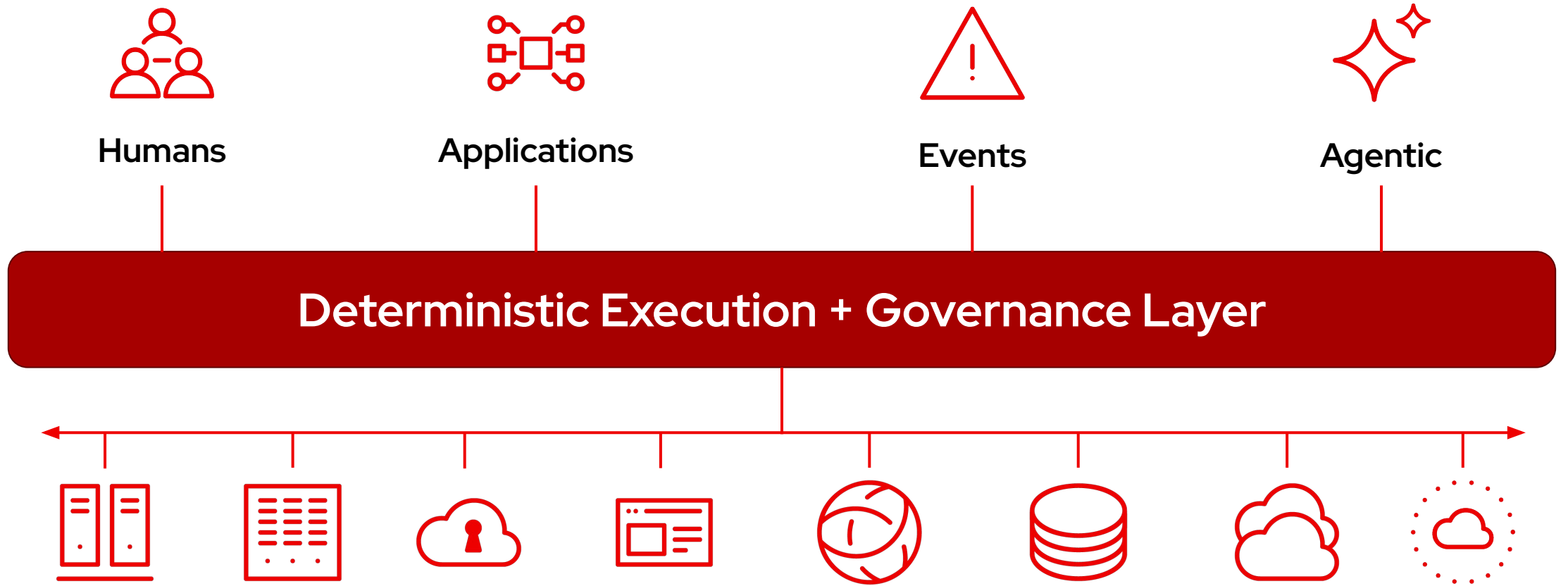


Challenging to explain – while the workings of non-agentic frontier AI systems are notoriously difficult to interpret, the range of behaviours and tools available to agents make it even more challenging to explain a particular course of action



Accelerating Defence

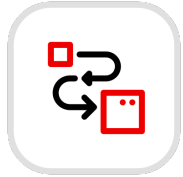
High Level Design





Red Hat
Ansible Automation
Platform

Automation Controller



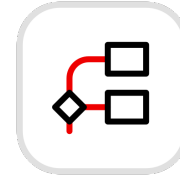
Workflow Engine
Focused on Ansible execution

- ▶ Executions are not durable
- ▶ No guarantee execution reaches certain state.
- ▶ Limited error handling & logic.
- ▶ Single user case automation.



Red Hat
Ansible Automation
Platform

Automation Orchestrator

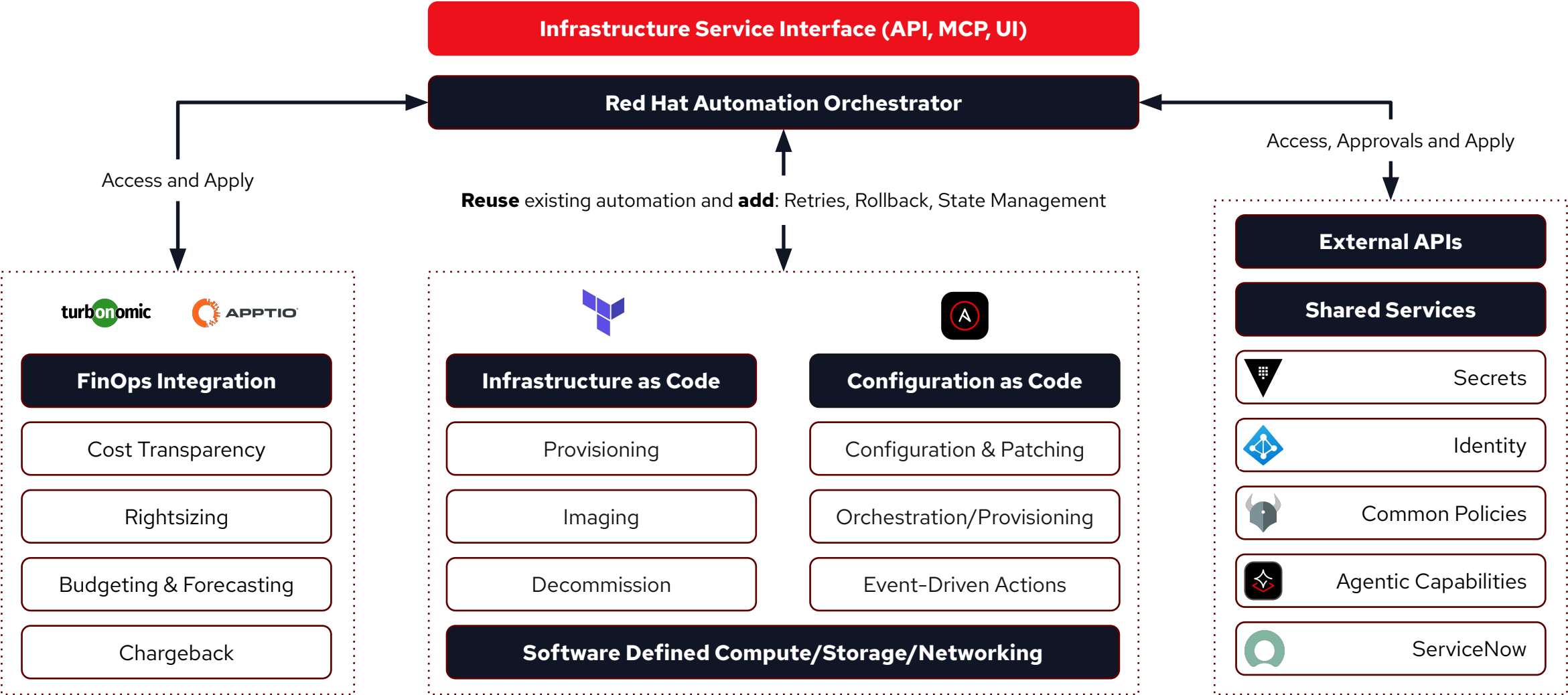


Orchestration Engine
Multi-stage, multi-tool, execution

- ▶ Durable workflows, maintains state for reruns.
- ▶ Guaranteed end state.
- ▶ Supports complex logic.
- ▶ Multi-stage execution.
- ▶ Can inject agentic behaviour.



Red Hat Automation Orchestrator





Vulnerability Remedia...



All projects ▾

Unpublished changes

⛶ Add Step

▶ Run

💾 Save

📄 Publish



Agents, events,
playbooks all
orchestrated on a
single canvas

Alerts from multiple sources

AI analyzes and recommends

Automated
remediation at scale



Legend



Steps



AI agent



Action



AAP execution



Logic



Approval



Trigger

Connectors



Approved



Rejected



IBM Instana Vulnerability
Alert

Event-Driven Ansible trigger



ServiceNOW
Vulnerability Alert

Event-Driven Ansible trigger



Splunk Vulnerability
Alert

Event-Driven Ansible trigger

Create SNOW Ticket

Job Template

Create SNOW Ticket



Vulnerability Analysis

Agentic

Model

gpt-4

Tools

4 tools



Human Review

Approval

Timeout

3600s

Approved

Rejected



Execute Remediation

Job Template

Patch and Restart

Events trigger
deterministic
automation rulebook

Humans approve

Capabilities to increase *velocity*

If you need...	Red Hat can show you how to...
Better Collaboration	get users to share content securely , and increase trust and collaboration.
Integrated ITSM	integrate EDA with your ITSM to accelerate ticket remediation
Cross Domain Workflows	securely orchestrate across domains .
Better Governance	use AAP Policy as Code to centralise automation compliance.
AIOps Guidance	use AI to augment and enhance existing automation workflows.
Self-Service	enable users to easily consume automation to speed up dev, test and ops.
Faster Time-to-market	speed up your automation content generation and upskill users.



References



AI slop pollutes the
CVE pipeline with
fake vulns



Zero Day Clock



Anthropic threat intelligence
report September 2026



Black Hat 2026
The Hugging Face
Incident



NCSC - Thinking
carefully before
adopting agentic AI



NCSC - Cyber Shield:
The path to an agentic
AI future for cyber
defence



British Army Case Study



Why collaboration is vital
for achieving
'automation nirvana'



Red Hat Automation
Orchestrator





Connect

Thank you



linkedin.com/company/red-hat



facebook.com/redhatinc



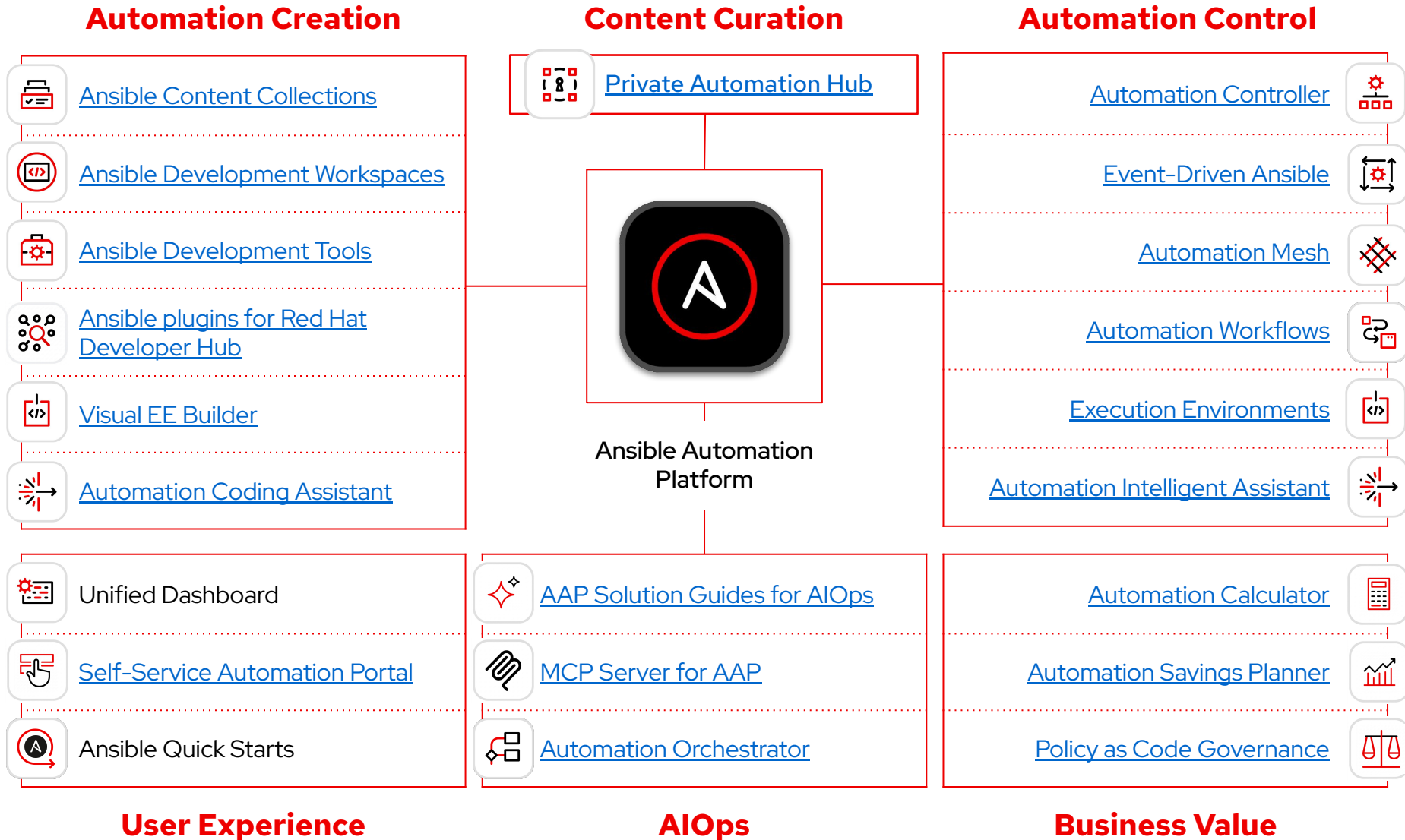
youtube.com/user/RedHatVideos



x.com/RedHat



Links to resources



AIOps latest resources

Read these articles/blogs/papers

- Digital: redhat.com/automation-aiops
- Article: [AIOps explained](#)
- Article: [The journey from observability to AIOps automation](#)
- Checklist: [5 practical AIOps use cases](#)
- Blog: [AIOps and Ansible Automation Platform: Where AI intelligence meets trusted execution](#)
- Blog: [IT automation with agentic AI: Introducing the MCP server for Red Hat Ansible Automation Platform](#)
- Solution Guides: [Ansible Automation Platform and AI](#)
- Market Research Paper: [Closing the AIOps Gap: Why AI Insights Need Trusted Action](#)

Check out these videos + webinars

- Webinar: [Turning Intelligence into Trusted Automation](#)
- Webinar: [AIOps to Action: Automating the Future of IT Operations](#)
- Video: [5 use cases with MCP server for AAP](#)
- Video: [How to setup Cursor to work with MCP server for AAP](#)
- Video: [How to setup Copilot Studio to work with MCP server for AAP](#)
- Video: [Automate Windows Certificate Rotation with Ansible + AI](#)
- Video: [AIOps: Patch RHEL CVEs in Minutes with Red Hat Lightspeed MCP and Ansible Automation Platform](#)

Solution Guides

Solution Guides

HomeAIOpsBest practicesOpen an issueSearch...

Filter by

Type

☐ Foundational

☐ Integration

Status

☐ Published

☐ Work in Progress

Partners

☐ AWS

☐ Azure

☐ EDB PostgreSQL

☐ IBM Instana

☐ Red Hat AI

☐ ServiceNow

☐ Splunk

Solution Guide

AIOps automation with Ansible

Self-healing infrastructure using Event-Driven Ansible, Red Hat AI inference, and Ansible Lightspeed to detect, diagnose, and remediate incidents automatically.

Foundational

Solution Guide

High-Availability AAP with EDB PostgreSQL DR

Multi-datacenter Active-Passive disaster recovery for Ansible Automation Platform using EDB Postgres Advanced Server and EDB Failover Manager with sub-5-minute RTO.



Solution Guide

Automated Incident Remediation with IBM Instana

Closed-loop incident remediation integrating IBM Instana observability with Event-Driven Ansible for automatic detection, AI-driven job template routing, and self-healing infrastructure.



Solution Guide

AI Infrastructure automation with Ansible

Provision and configure Red Hat AI infrastructure -- from GPU instances to serving models -- using the infra.ai and redhat.ai collections.



Solution Guide

Intelligent Assistant with Red Hat AI Inference Server

Deploy and configure a self-hosted LLM using Red Hat AI Inference Server on RHEL with GPU acceleration to power the Ansible Lightspeed intelligent assistant in AAP.



Solution Guide

AIOps with Splunk and Event-Driven Ansible

Three use cases for closed-loop AIOps: ITS1 predictive anomaly detection with MLTK, RHEL server remediation with AI-enriched diagnostics, and network OSPF remediation with Lightspeed-generated playbooks.



red.ht/ansible-aiops



- ✓ Docs as code (Stored on Github)
- ✓ Detailed walkthroughs

