Red Hat Summit

Connect

The Mythos Era: patching at the speed of AI

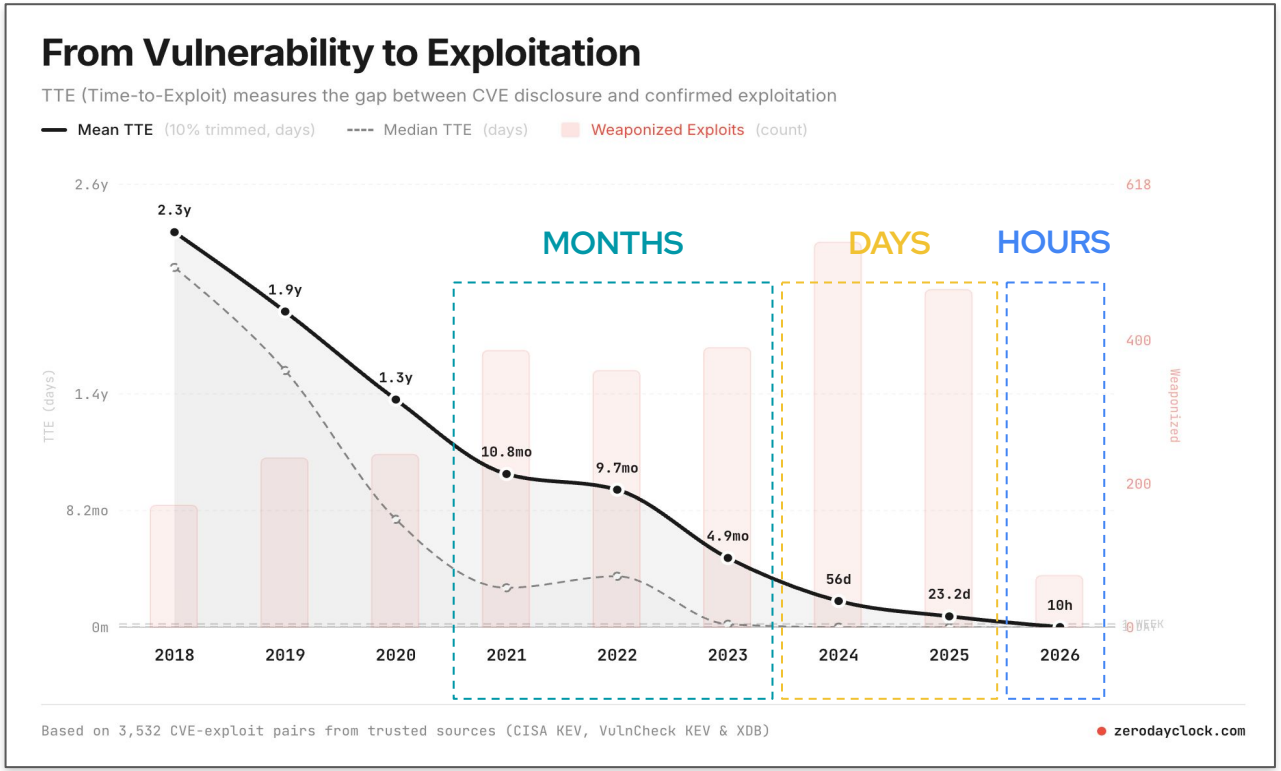
Enterprise IT Automation in an AI-Accelerated Threat Landscape

Darren Long
Enterprise Automation Specialist

Jens Boivie
Specialist Solution Architect

Red Hat

AI is Accelerating the Security Vulnerability Landscape



Mythos Threats to Customers

- Automate Exploitations
- Chaining Vulnerabilities
- Expose Critical Infrastructure
- Increase Threat Volume
- Increase Threat Velocity
- Lower Barrier to Entry

Source: The "AI Vulnerability Storm": Building a Mythos-ready Security Program, Zero Day Clock

Red Hat | IBM

What's the latest?

Rapid7 · Q3 2026

3 days

Average time from disclosure to observed exploitation of high-severity vulnerabilities

Rapid7 · Q3 2026

71%

Of tracked exploitation occurred within the first seven days

Microsoft · October 1, 2026

<24 hrs

Median time from vulnerability discovery in the wild to weaponisation

Microsoft · October 1, 2026

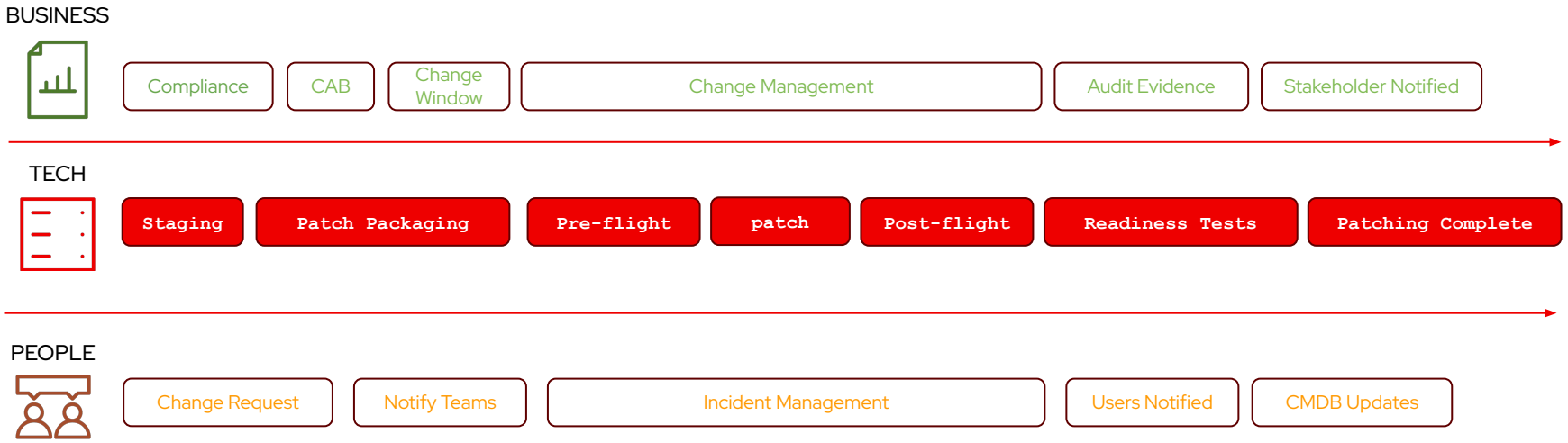
30–60 days

Enterprise remediation time for critical externally exposed vulnerabilities

Sources: Rapid7 Q3 Threat Landscape Report and Microsoft Digital Defense Report 2026


YOUR SOFTWARE
CVE
(vulnerability)
PATCH
(Fix)
IT Ops
Identify CVEs
Test
Deploy patch
Verify
CVE
CLOSED
(Protected)

It’s more than just tech



Automate to stay ahead of threats in the AI era



Speed

From weeks to hours for configuration mitigation and critical patches. Reduces exposure window by 90%+.



Scale

Handle thousands of vulnerabilities. Orchestrate across global hybrid infrastructure.





Intelligence

Supports context-aware prioritization and recommendations for threat mitigation



Governance

Audit trails for every action. Role-based access and change management.

Red Hat

The Integrated Workflow

Close the Gap Between Discovery and Remediation

MITIGATE	PATCH	VALIDATE	VERIFY
Deploys targeted controls at scale when patches aren't available—breaking exploit chains in hours.	Orchestrates validated patching across hybrid infrastructure with governance and rollback.	Confirms the patch closes the vulnerability without introducing regression before production deployment.	Maintains continuous compliance, prevents drift, and provides complete audit trails.



Network



Operating systems



Cloud



Virtualization



Application delivery



AIOps

Red Hat

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 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.

This is not a Scary Problem.

This is a Scale Problem.

Defence in depth still works.

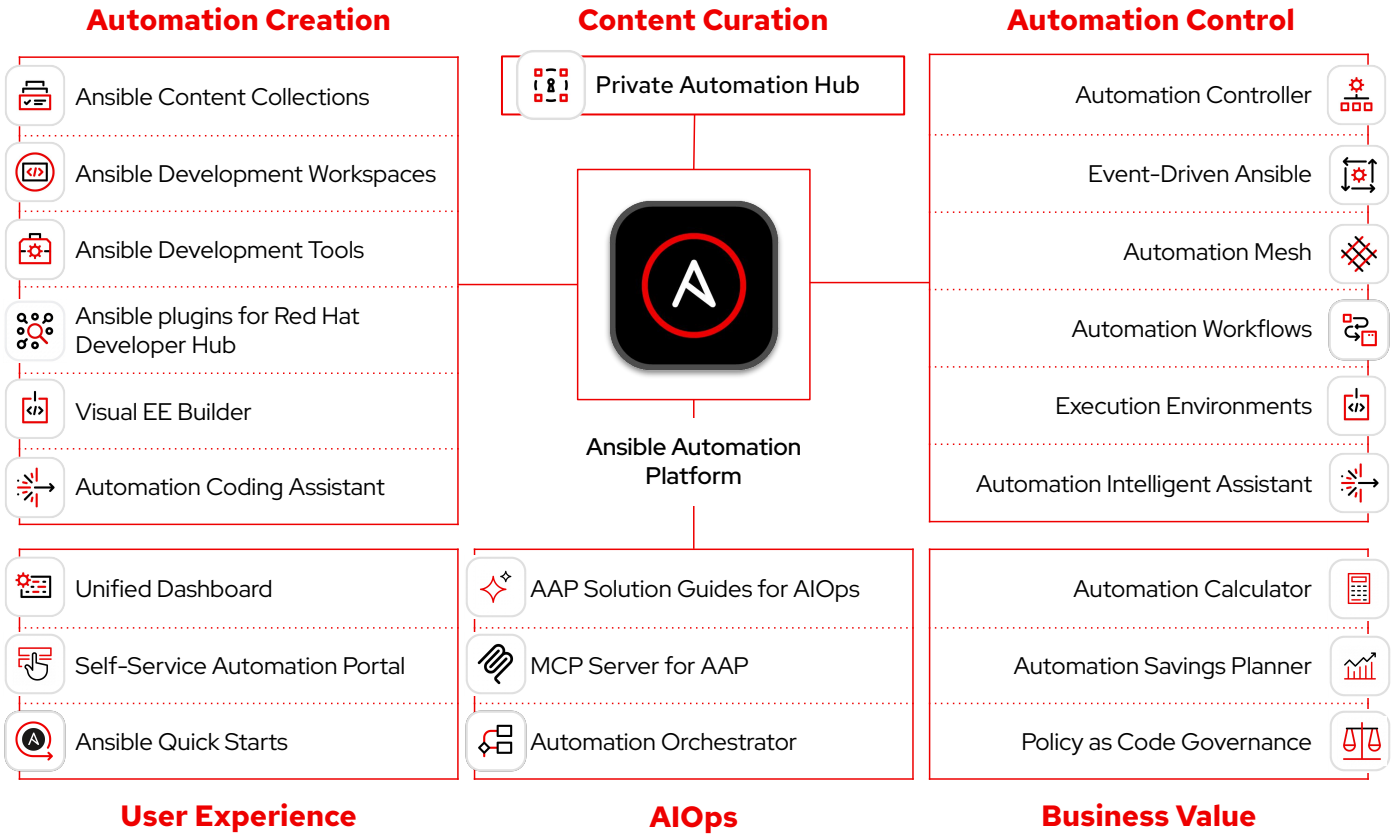
Patching still works.

Can you apply mitigation or remediation at machine speed?

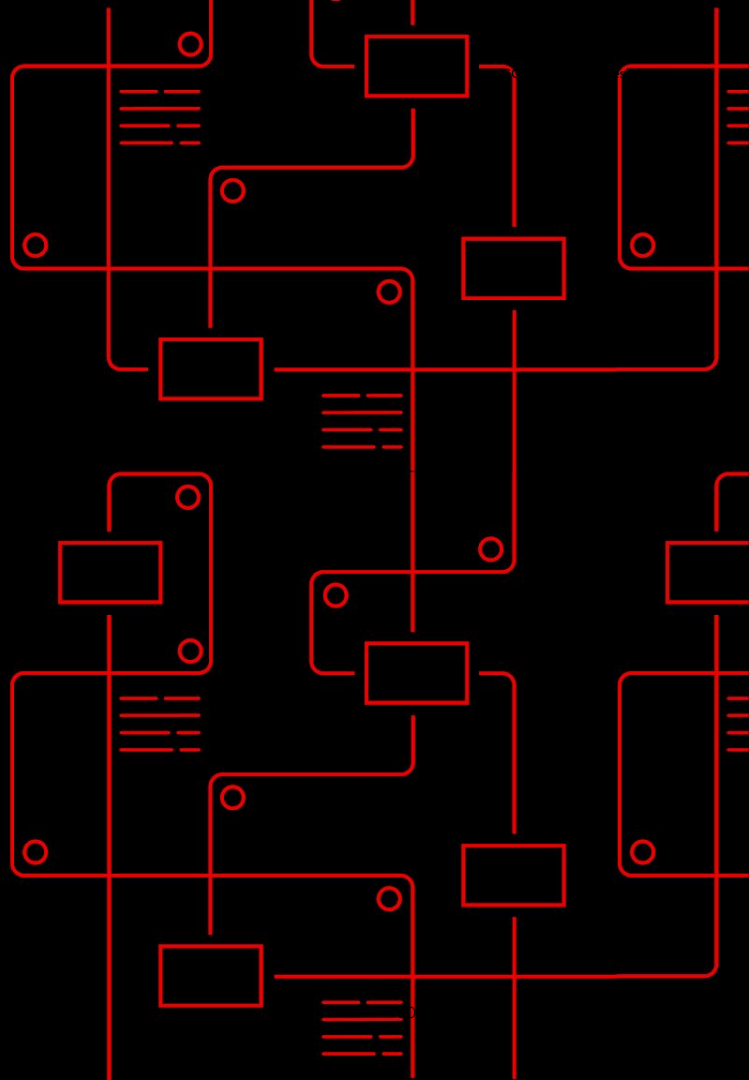
45% of vulnerabilities in large organisations remain unpatched after 12 months.

Source: Centre for Emerging Technology and Security (Alan Turing Institute), 2025 – cited in CETAS analysis, April 2026.

An integrated solution for the enterprise.

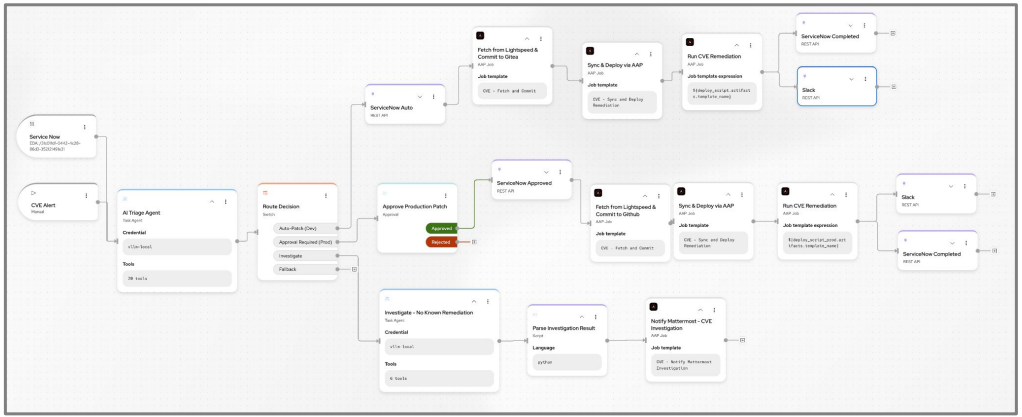


Demo



Demo. CVE Remediation

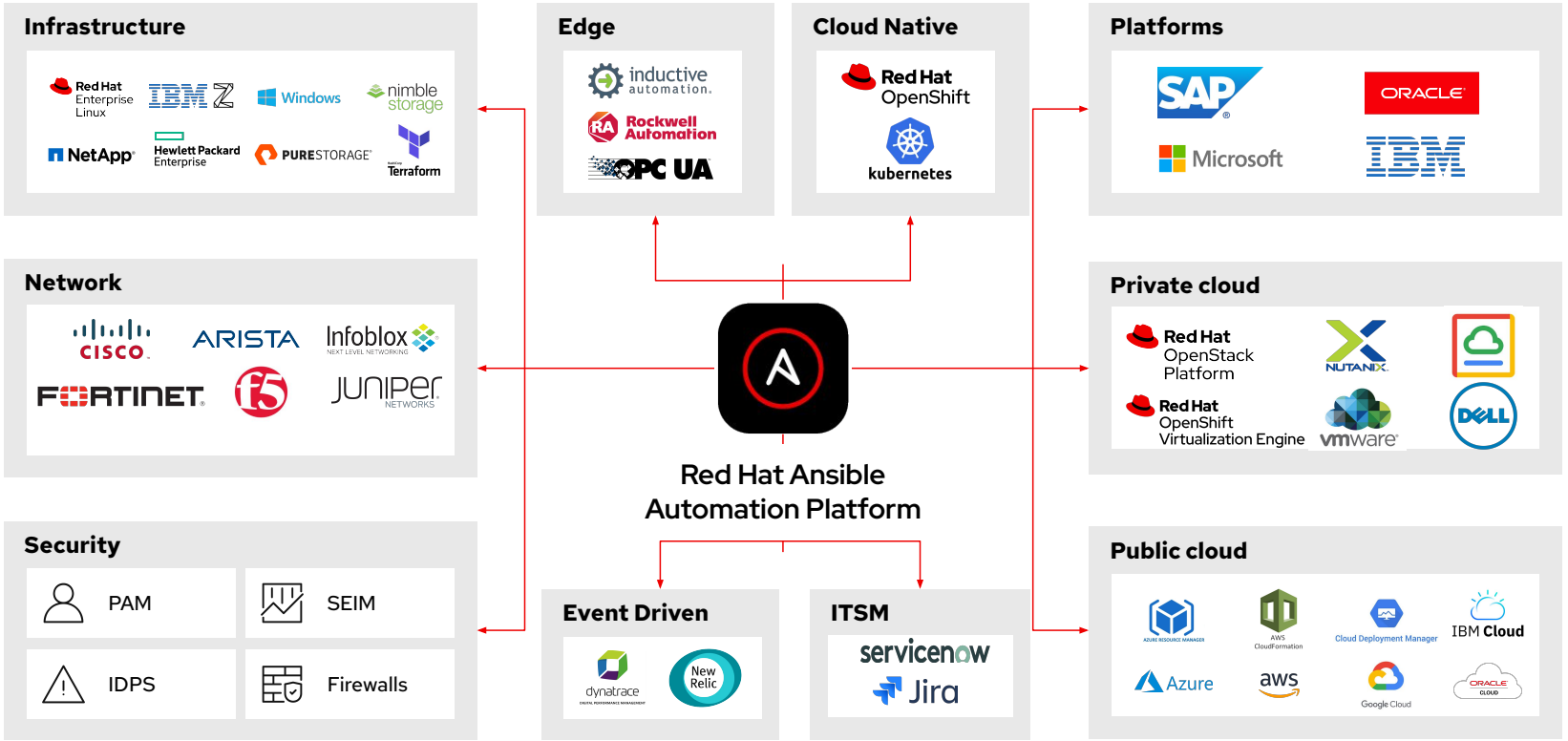
- Multiple triggers for same workflow
- AI Agent
- Red Hat Lightspeed Integration
  - Get remediation Ansible Playbook
- ServiceNow Integrations
  - Trigger
  - Service Request
  - Provide Service
  - Completed
- Slack Intergration
  - Post on Slack channel when done



Red Hat

200+ Certified and validated Content Collections

80+ Certified technology partners



Red Hat Ansible Automation Platform





Thank you!

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

linkedin.com/company/red-hat

facebook.com/redhatinc

youtube.com/user/RedHatVideos

twitter.com/RedHat

Red Hat