



Connect

Mitigación y Remediación automática de CVEs con Ansible y OpenShift IA

AI Ops on Security

Carlos Parada

Senior Specialist Solution
Architect (*Ansible*)

Nelson Paez

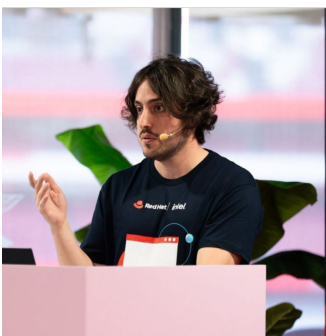
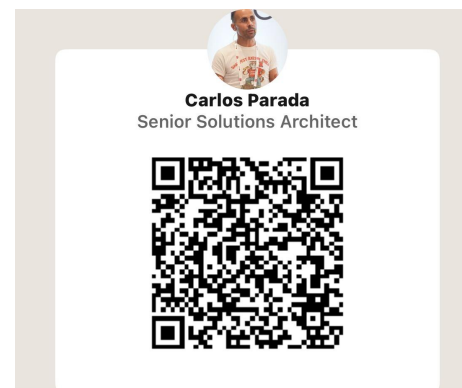
Specialist Solution
Architect (*Openshift AI*)





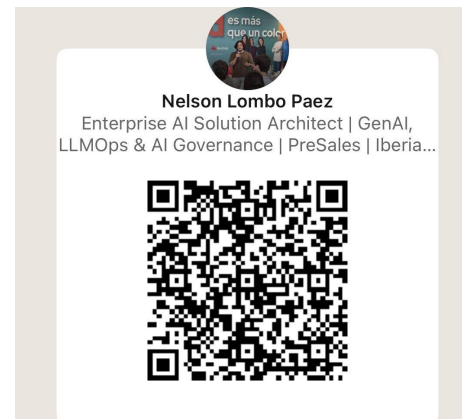
Carlos Parada

Senior Specialist Solution Architect (*Ansible*)
Red Hat



Nelson Paez

Specialist Solution Architect (*Openshift AI*)
Red Hat

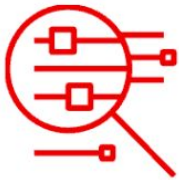


Security Moment



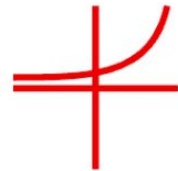
The Mythos Moment

When discovery outpaces defense



AI discovers vulnerabilities at machine speed

Frontier models find critical zero-day vulnerabilities autonomously — including bugs hidden for 27 years — at under \$50 each.



Vulnerability discovery now exceeds remediation capacity

Discovery is exponential. Remediation is linear.

Less than 1% of AI-discovered vulnerabilities have been patched.



Discovery is no longer the bottleneck. Response is.

4.8M Unfilled cyber roles. Growing 19% year over year.

The National Vulnerability Database is shifting to selective enrichment.



Shift from vulnerability management to exposure management.

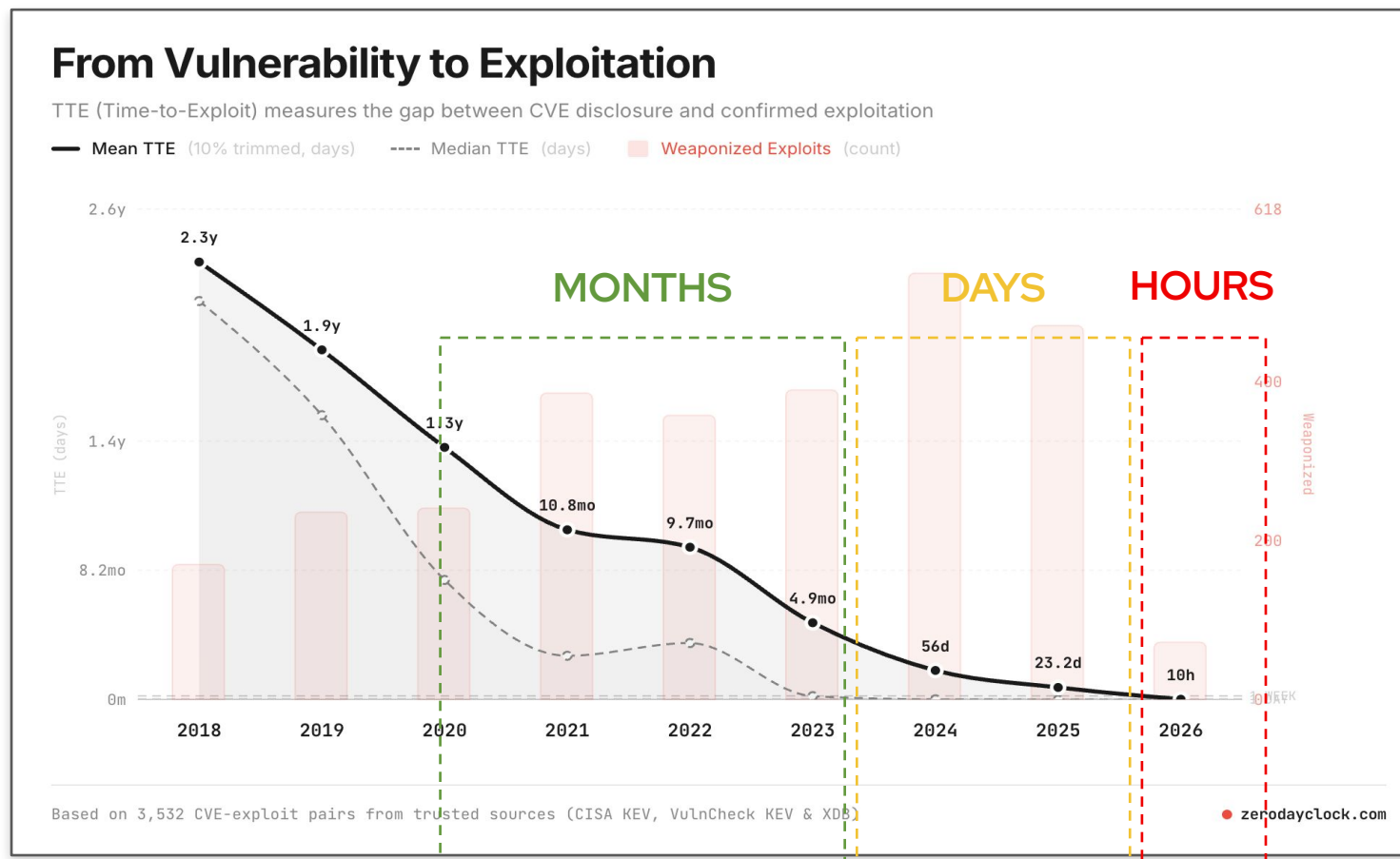
The number of published CVEs has grown more than 520% since 2016.

Cost of attacks in 2025 was ~\$60B. That's projected to grow to \$138B by 2031.



AI is Accelerating the Security Vulnerability Landscape

From Vulnerability to Exploitation



Mythos Threats to Customers

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



The integrated workflow

Mitigate, Patch, Validate and Verify

Close the Gap Between Discovery and Remediation

MITIGATE

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

PATCH

Orchestrates validated patching across hybrid infrastructure with governance and rollback.

VALIDATE

Confirms the patch closes the vulnerability without regression before production.

VERIFY

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



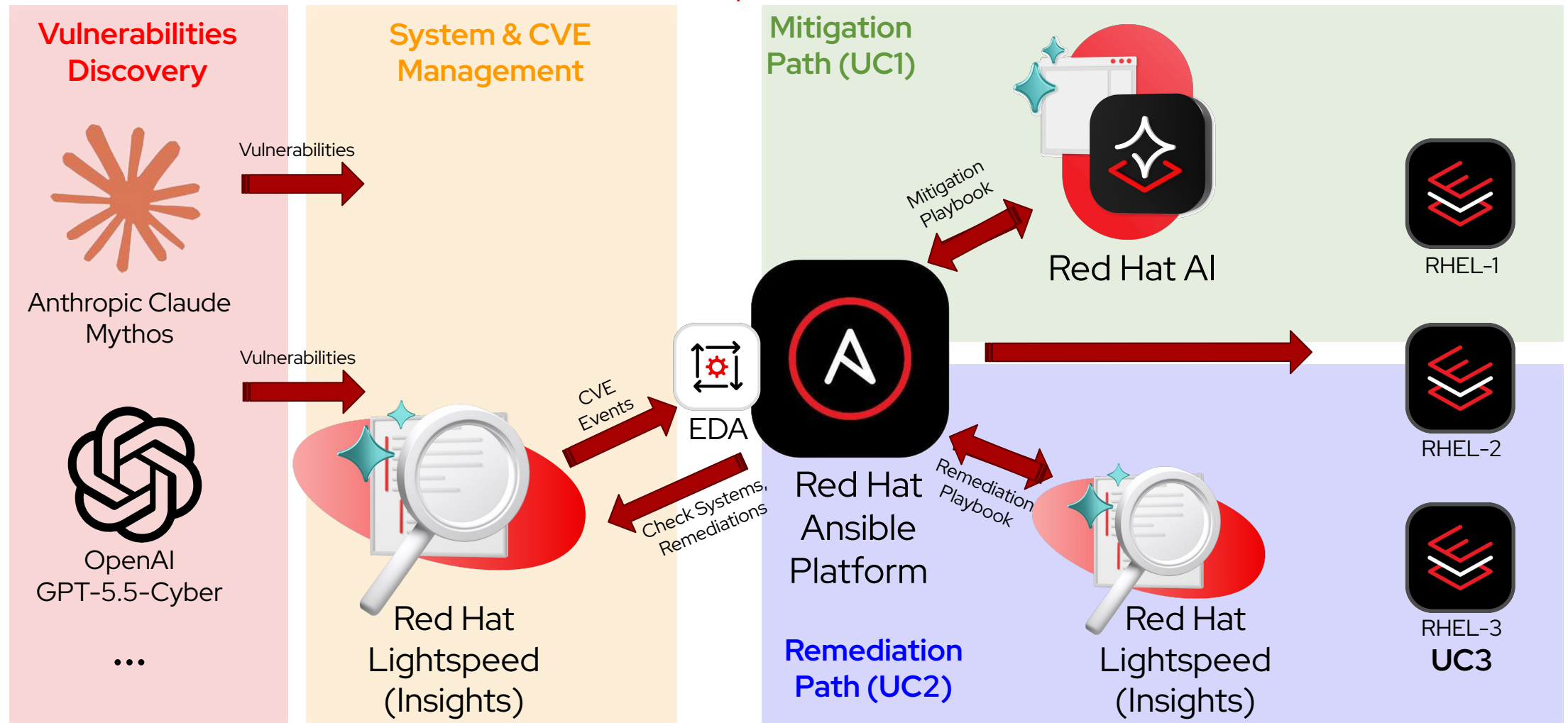
Demo

AI Ops: Mitigation and
Remediation of CVEs using
Red Hat Ansible and Red Hat AI



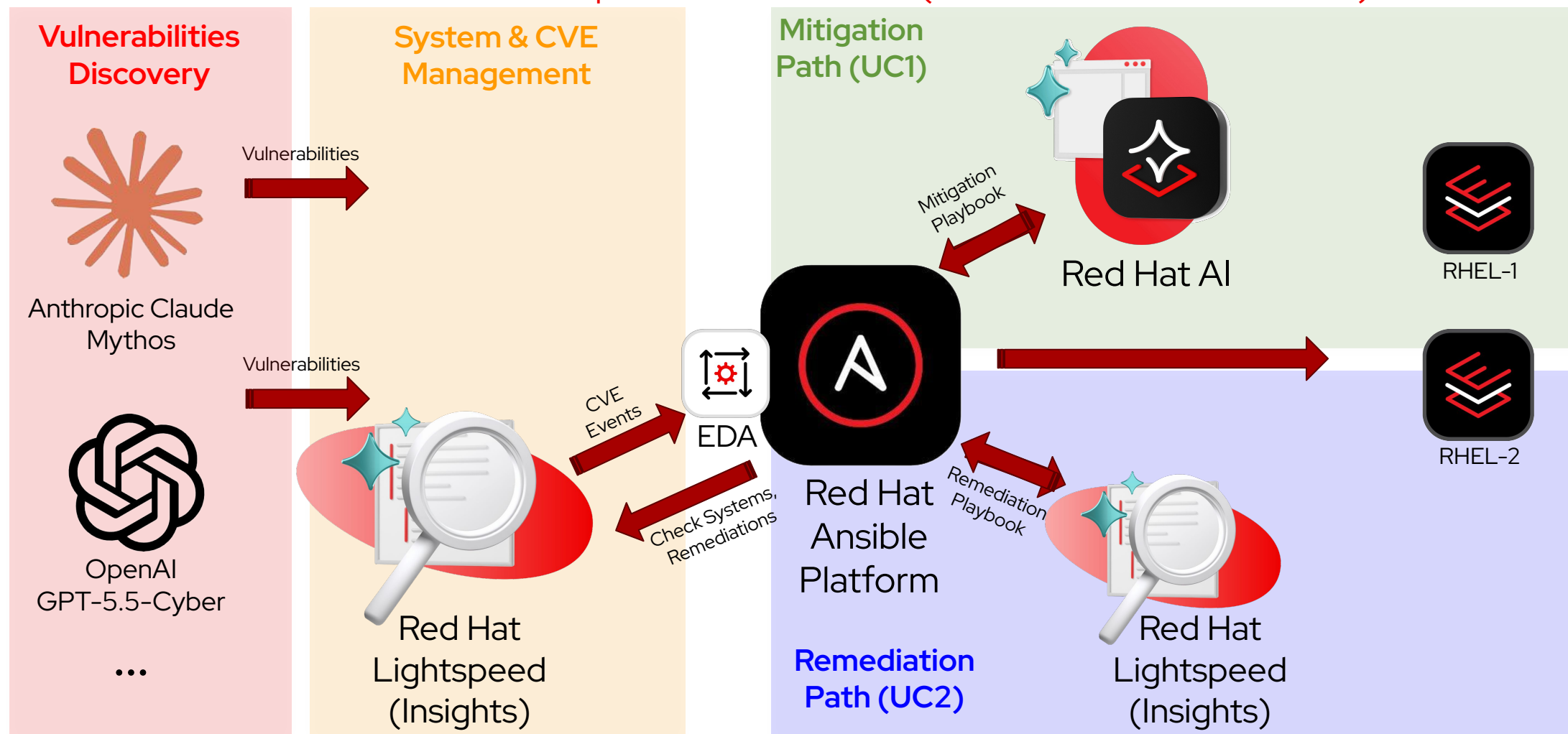
AIOps: Mitigation and Remediation of CVEs

AIOps Workflow



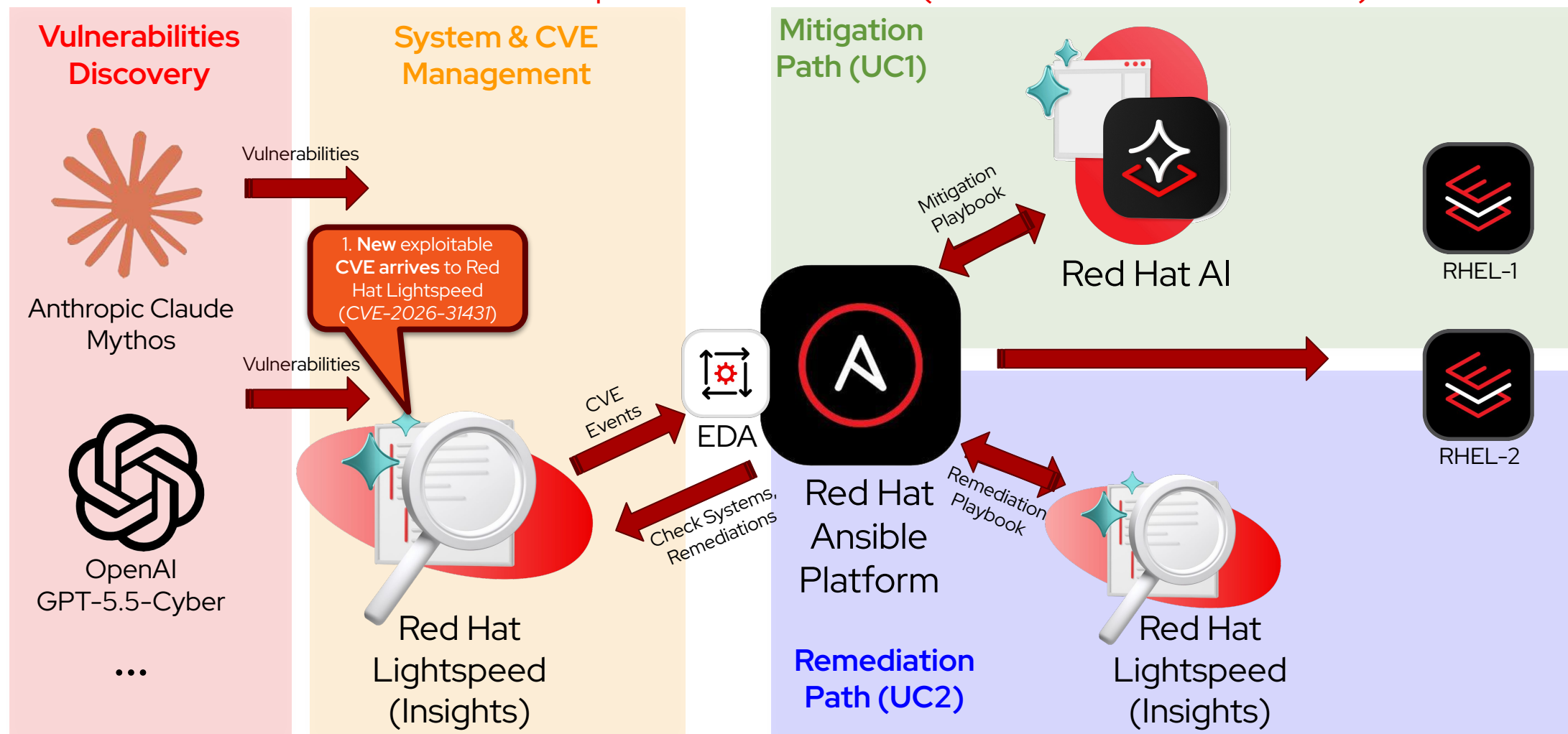
AIOps: Mitigation and Remediation of CVEs

Use Case 1 & 2: New exploitable CVE arrives (with or without Remediation)



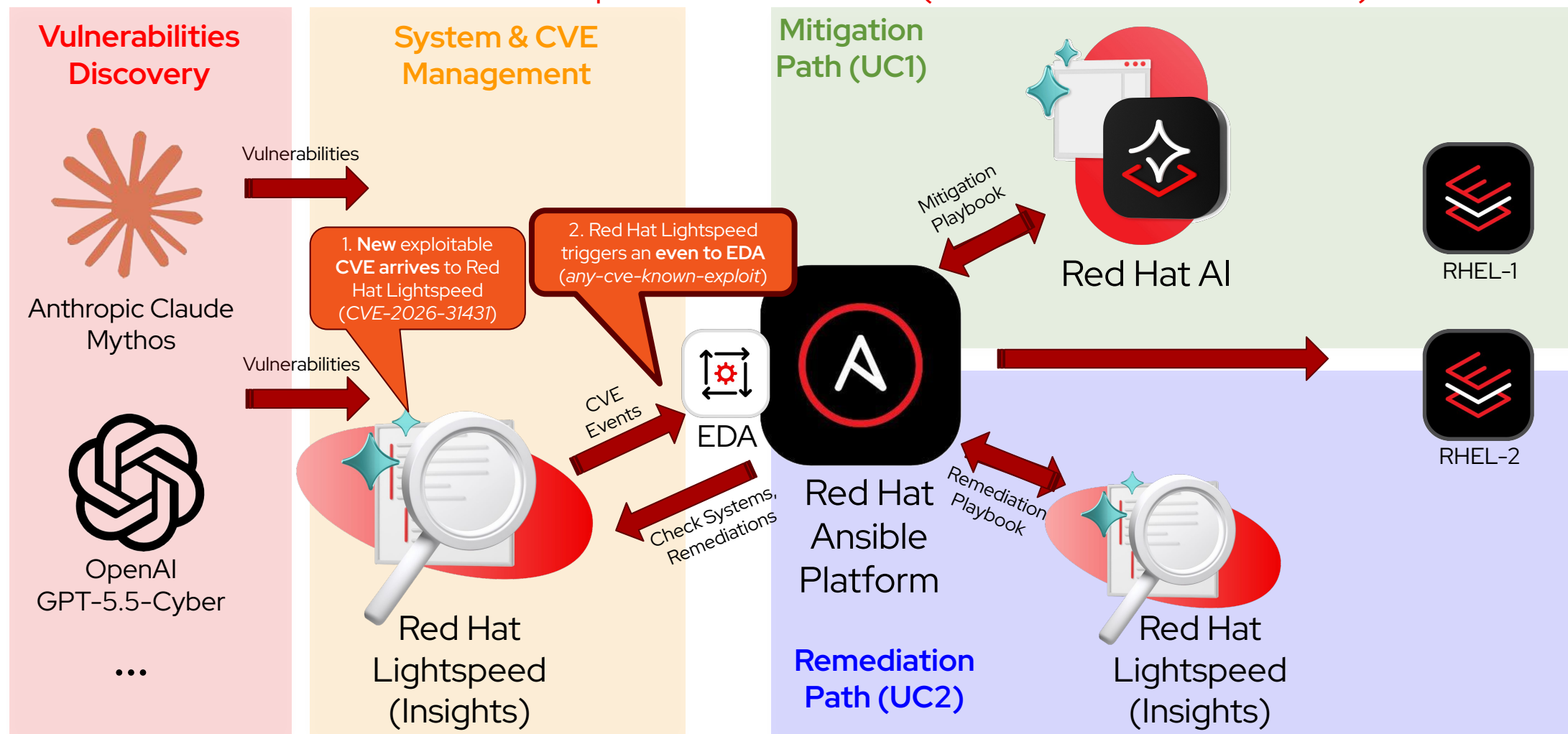
AIOps: Mitigation and Remediation of CVEs

Use Case 1 & 2: New exploitable CVE arrives (with or without Remediation)



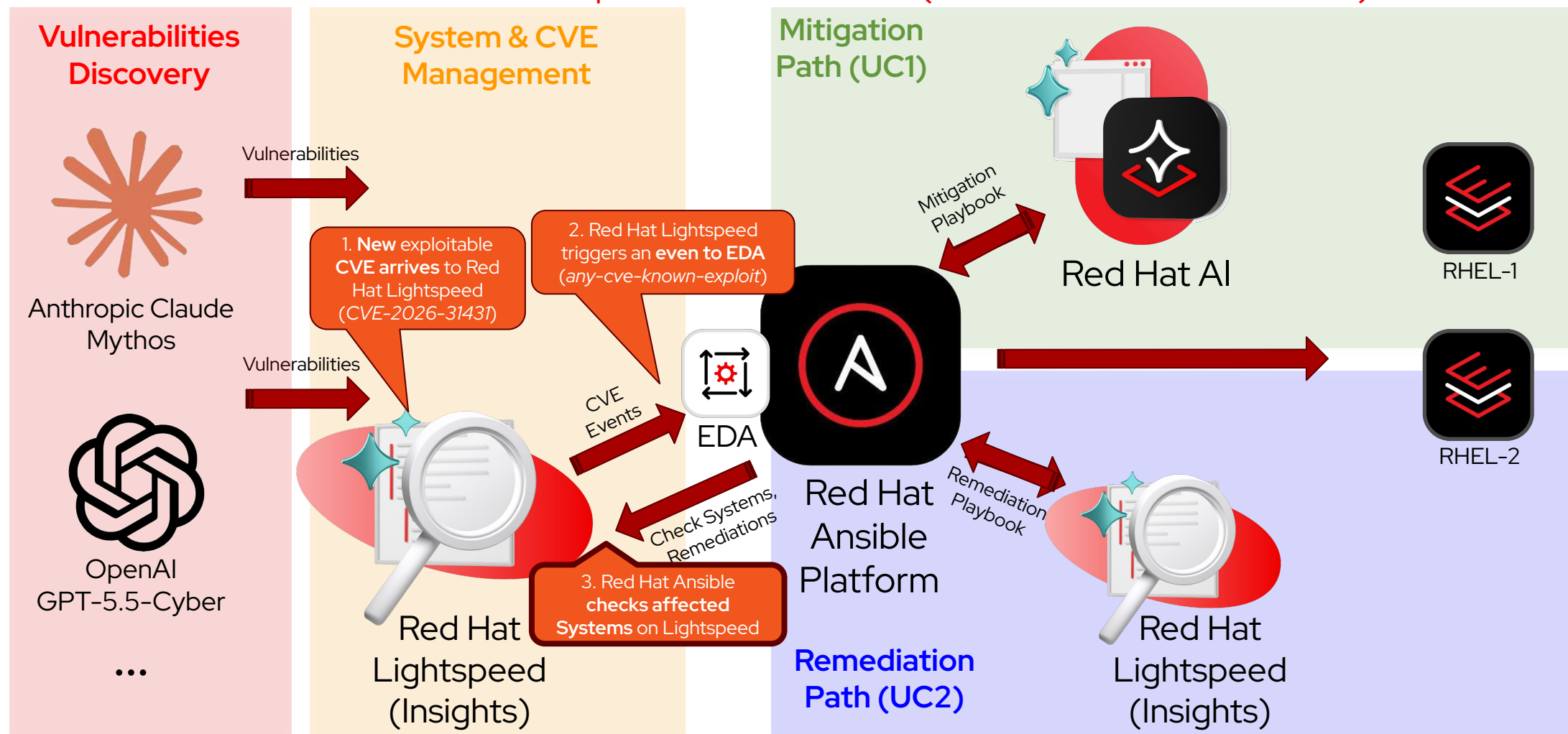
AIOps: Mitigation and Remediation of CVEs

Use Case 1 & 2: New exploitable CVE arrives (with or without Remediation)



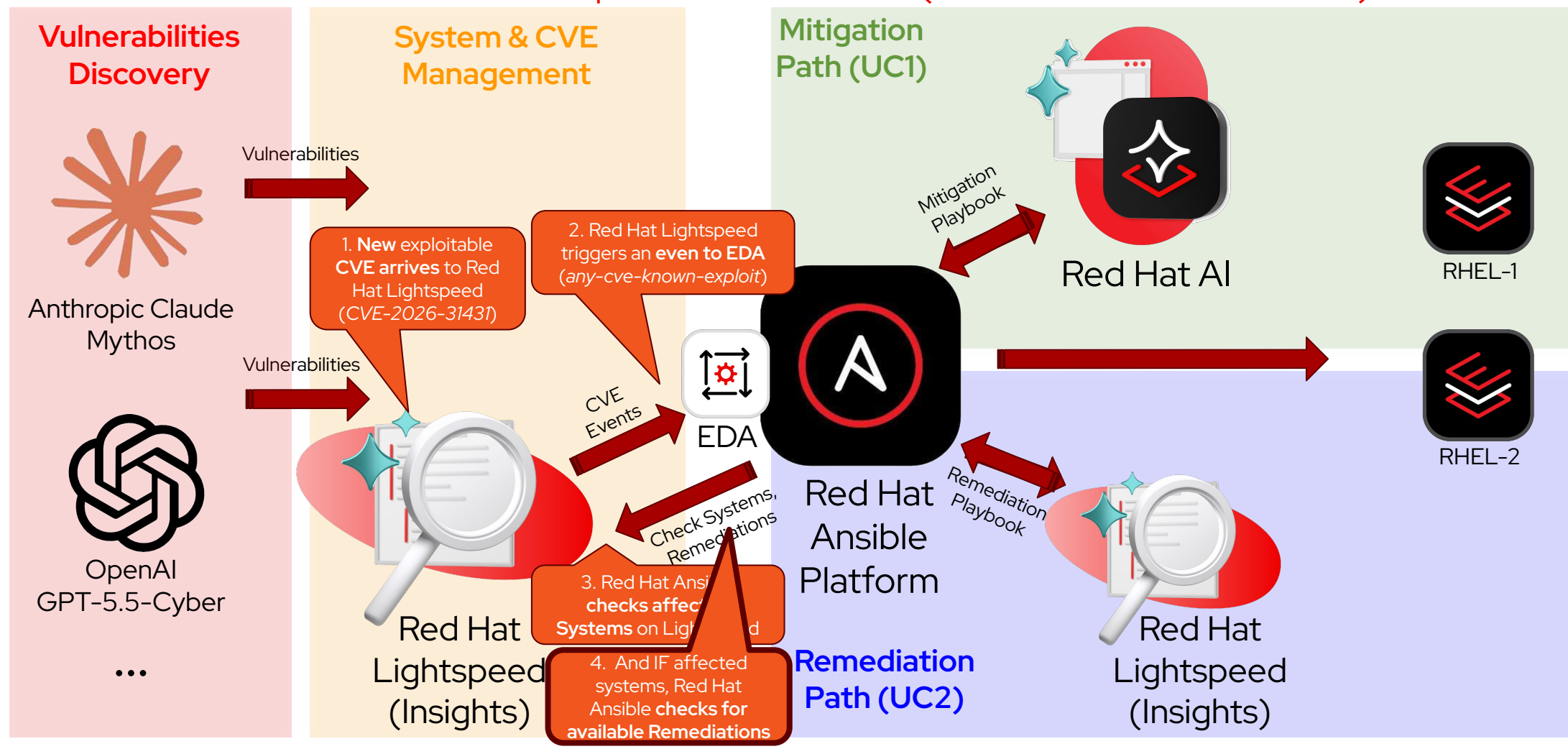
AIOps: Mitigation and Remediation of CVEs

Use Case 1 & 2: New exploitable CVE arrives (with or without Remediation)



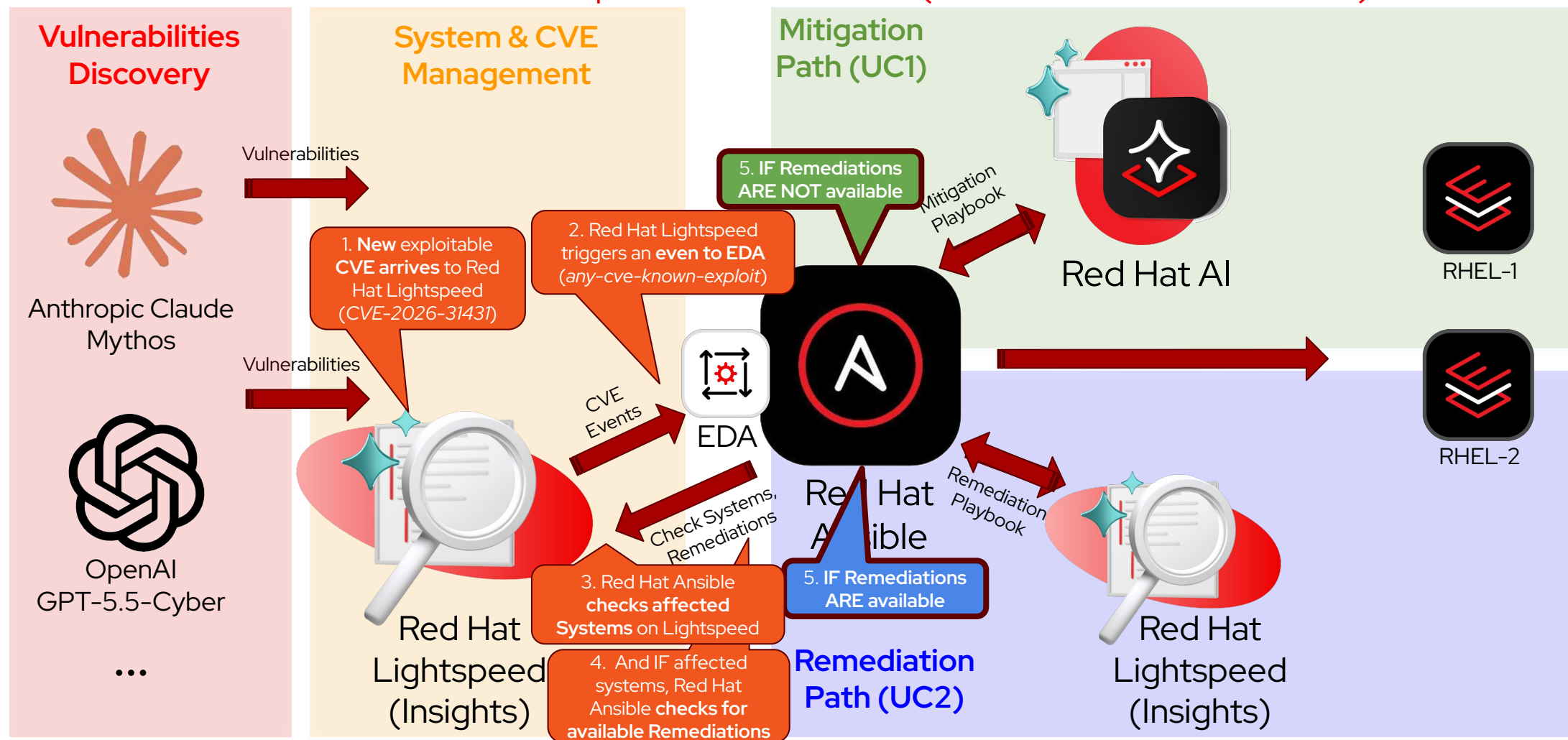
AIOps: Mitigation and Remediation of CVEs

Use Case 1 & 2: New exploitable CVE arrives (with or without Remediation)



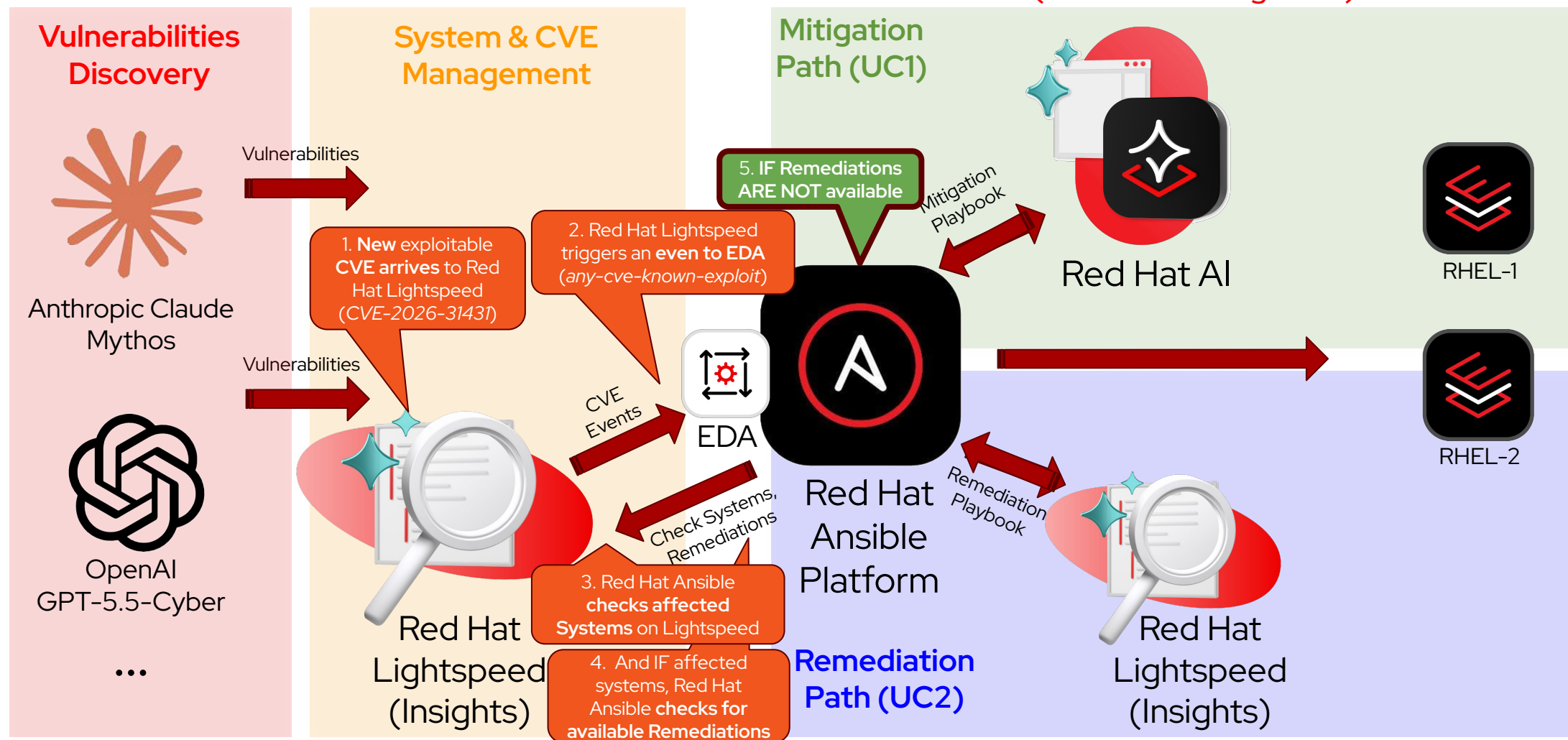
AIOps: Mitigation and Remediation of CVEs

Use Case 1 & 2: New exploitable CVE arrives (with or without Remediation)



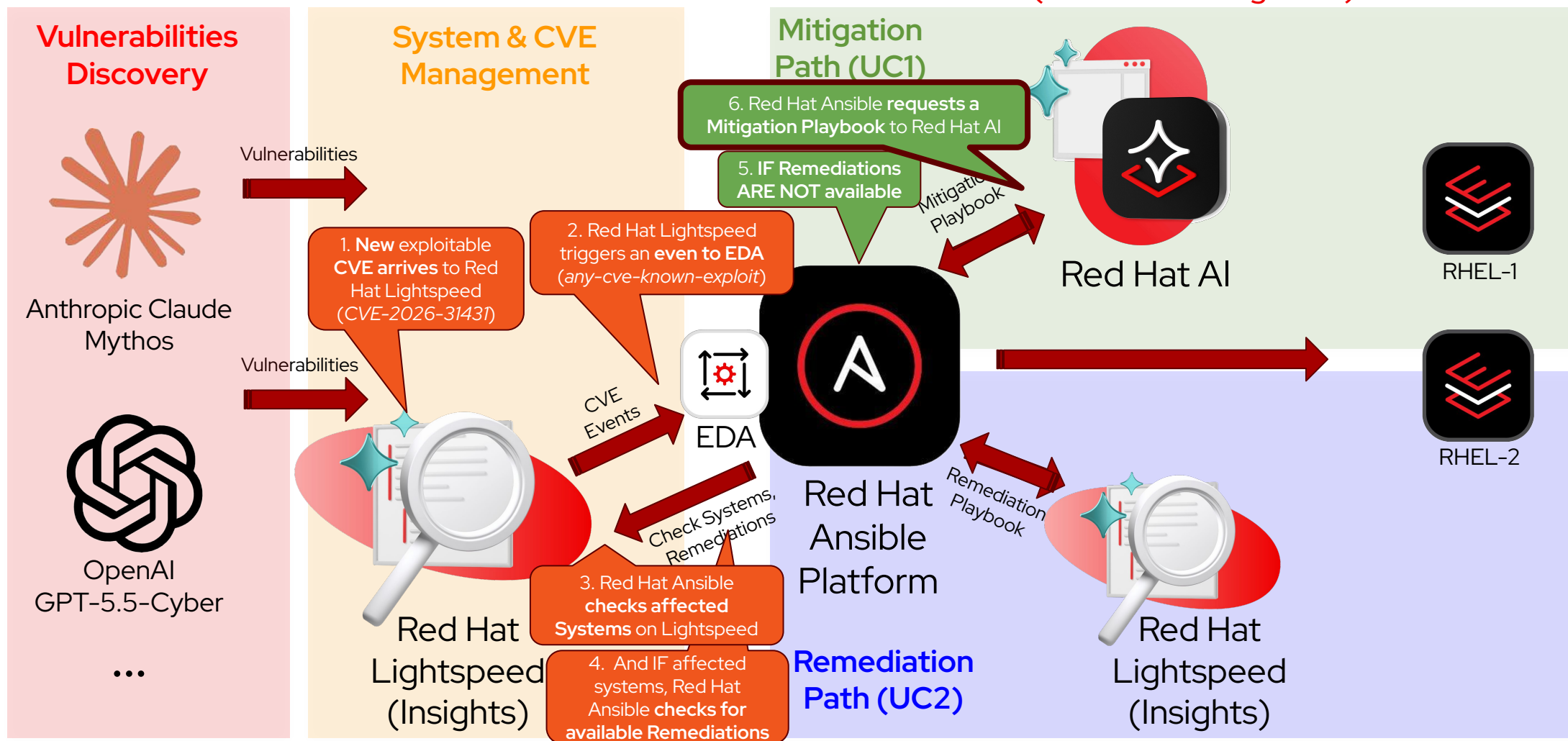
AIOps: Mitigation and Remediation of CVEs

Use Case 1: New CVE arrives with NO Remediation (AI-based Mitigation)



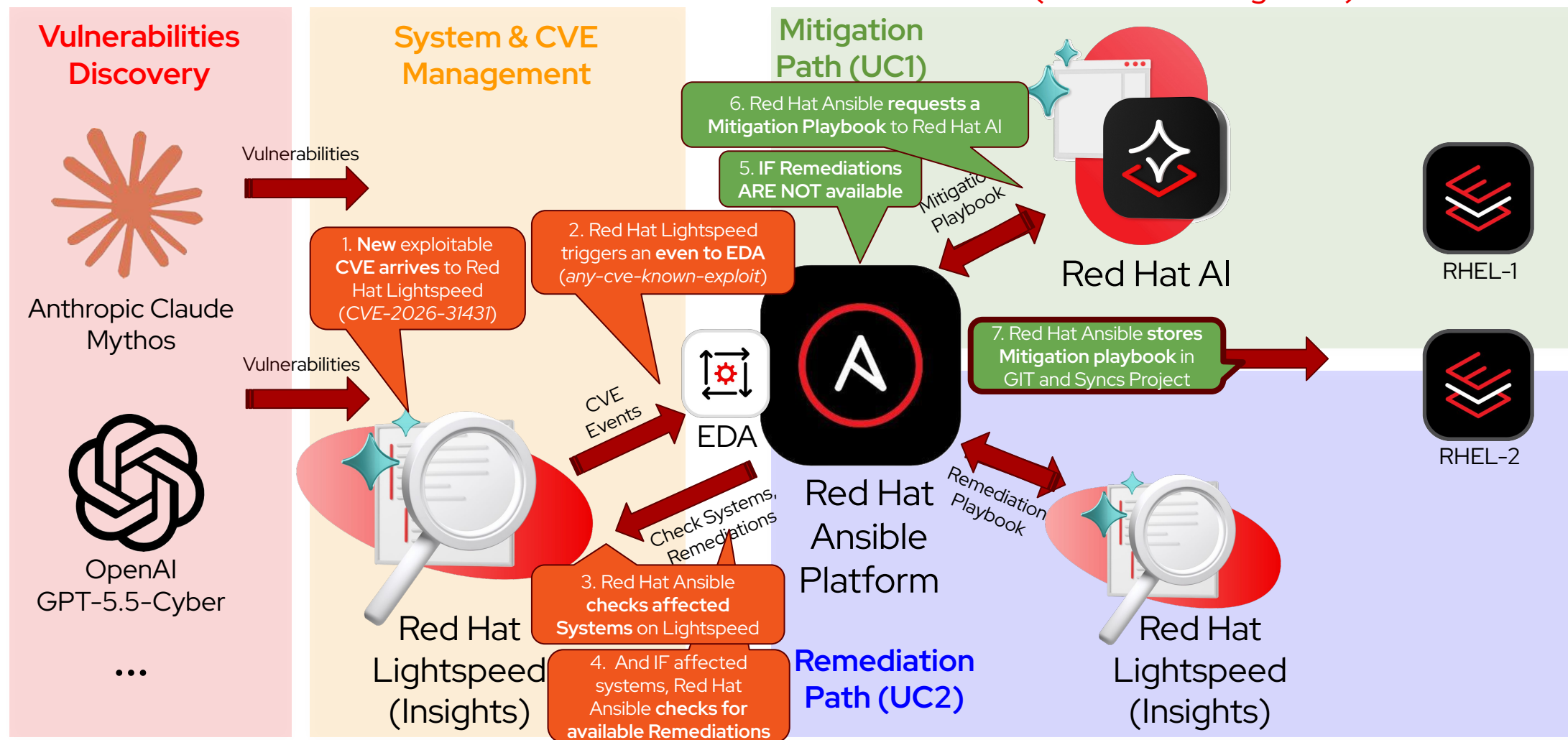
AIOps: Mitigation and Remediation of CVEs

Use Case 1: New CVE arrives with NO Remediation (AI-based Mitigation)



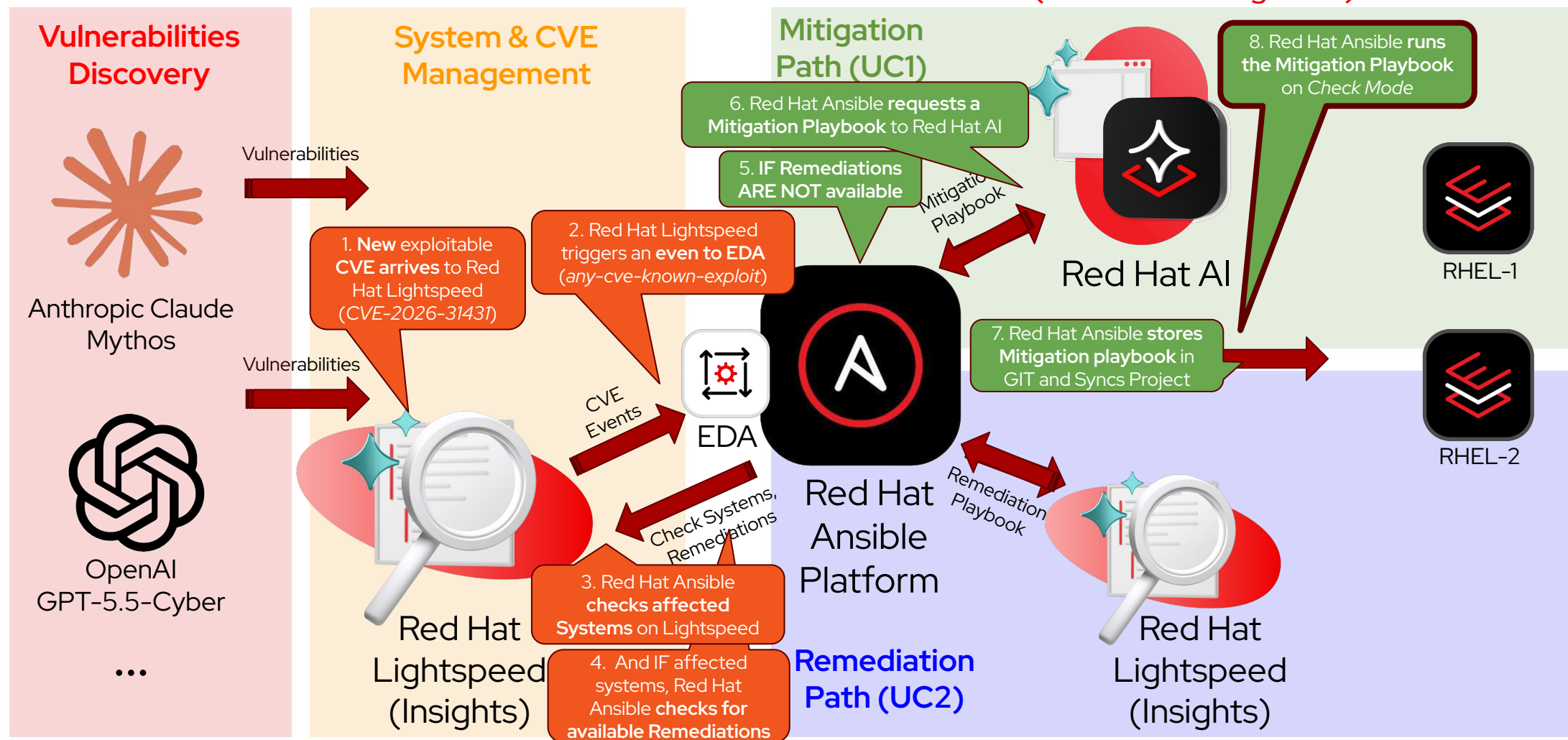
AIOps: Mitigation and Remediation of CVEs

Use Case 1: New CVE arrives with NO Remediation (AI-based Mitigation)



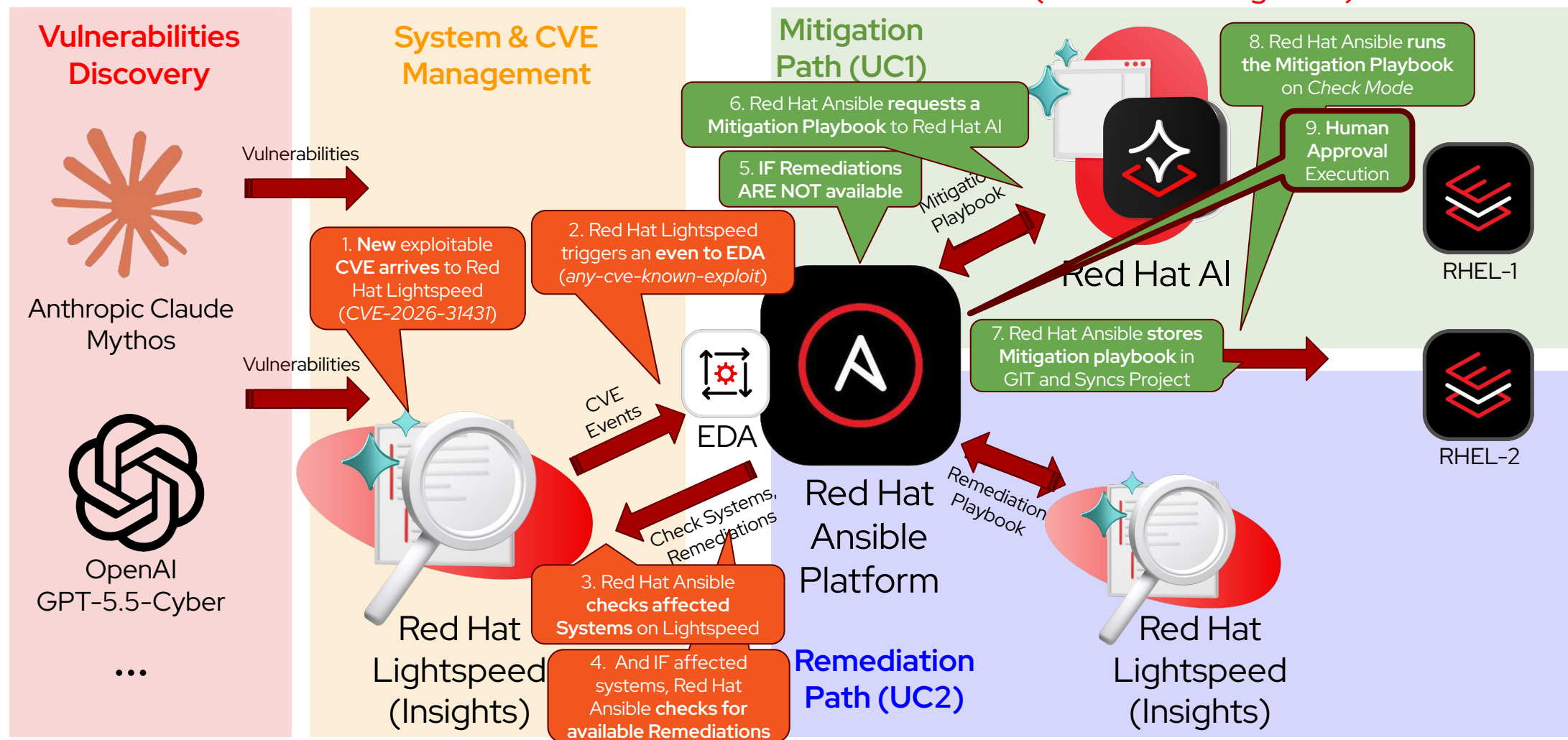
AIOps: Mitigation and Remediation of CVEs

Use Case 1: New CVE arrives with NO Remediation (AI-based Mitigation)



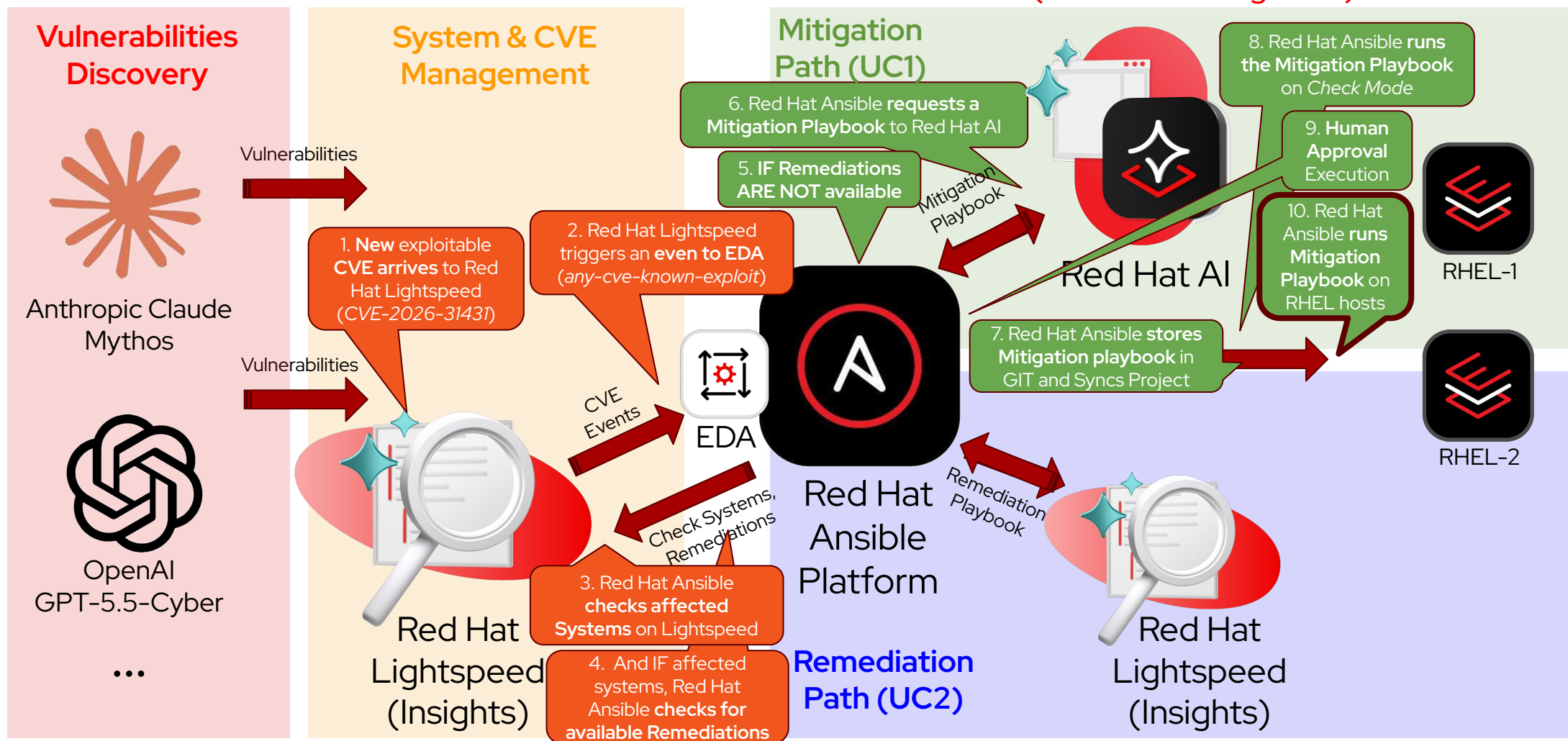
AIOps: Mitigation and Remediation of CVEs

Use Case 1: New CVE arrives with NO Remediation (AI-based Mitigation)



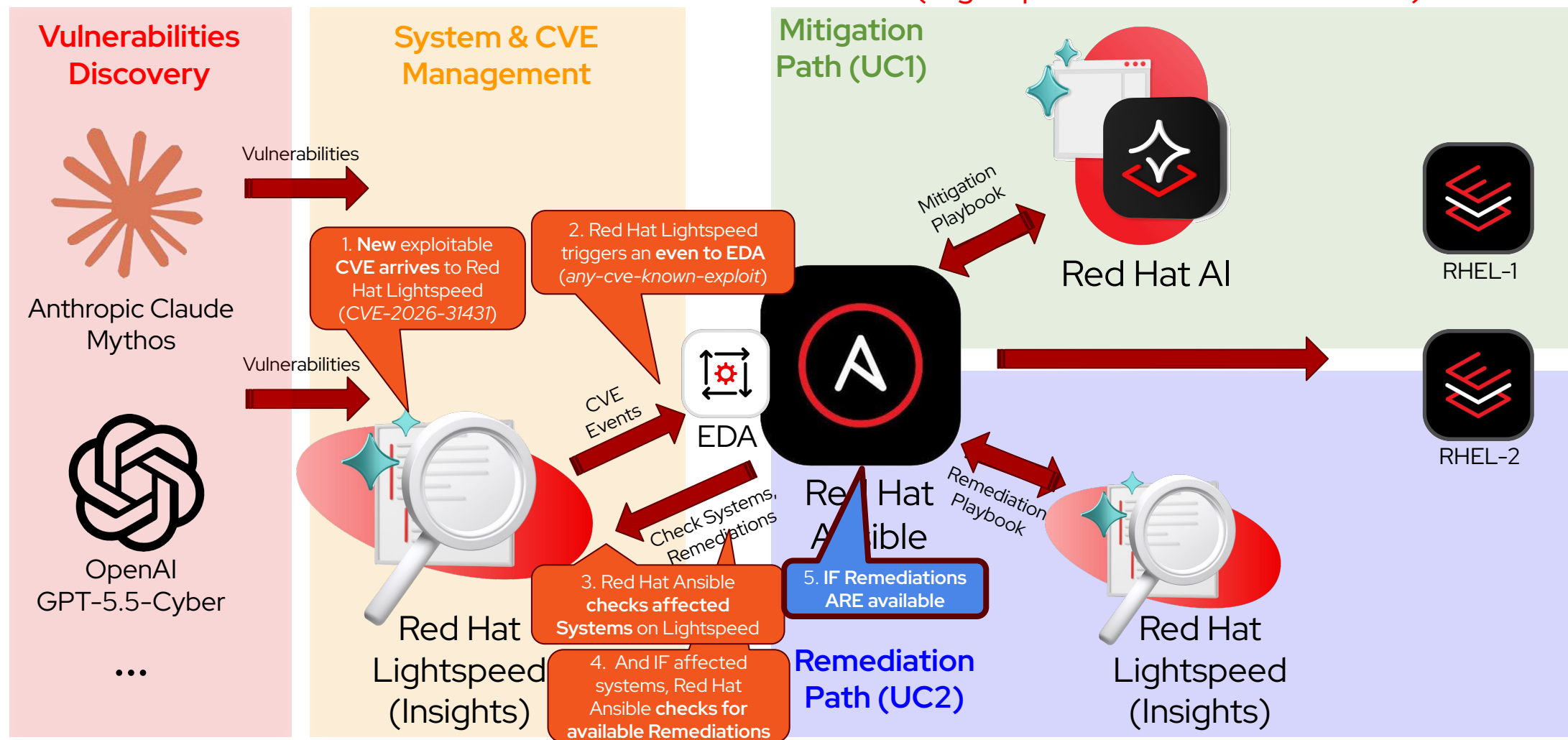
AIOps: Mitigation and Remediation of CVEs

Use Case 1: New CVE arrives with NO Remediation (AI-based Mitigation)



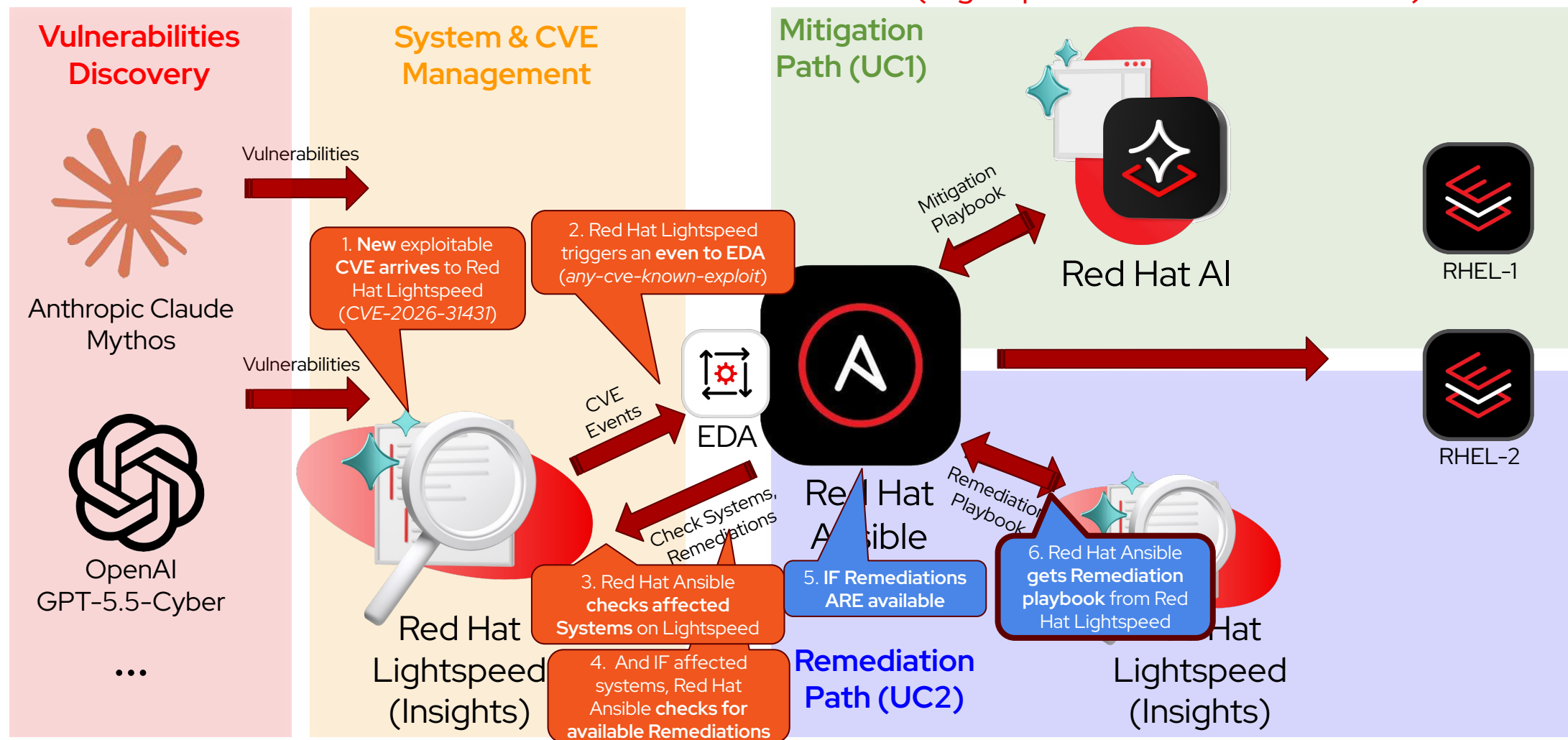
AIOps: Mitigation and Remediation of CVEs

Use Case 2: New CVE arrives with Remediation (Lightspeed-based Remediation)



AIOps: Mitigation and Remediation of CVEs

Use Case 2: New CVE arrives with Remediation (Lightspeed-based Remediation)

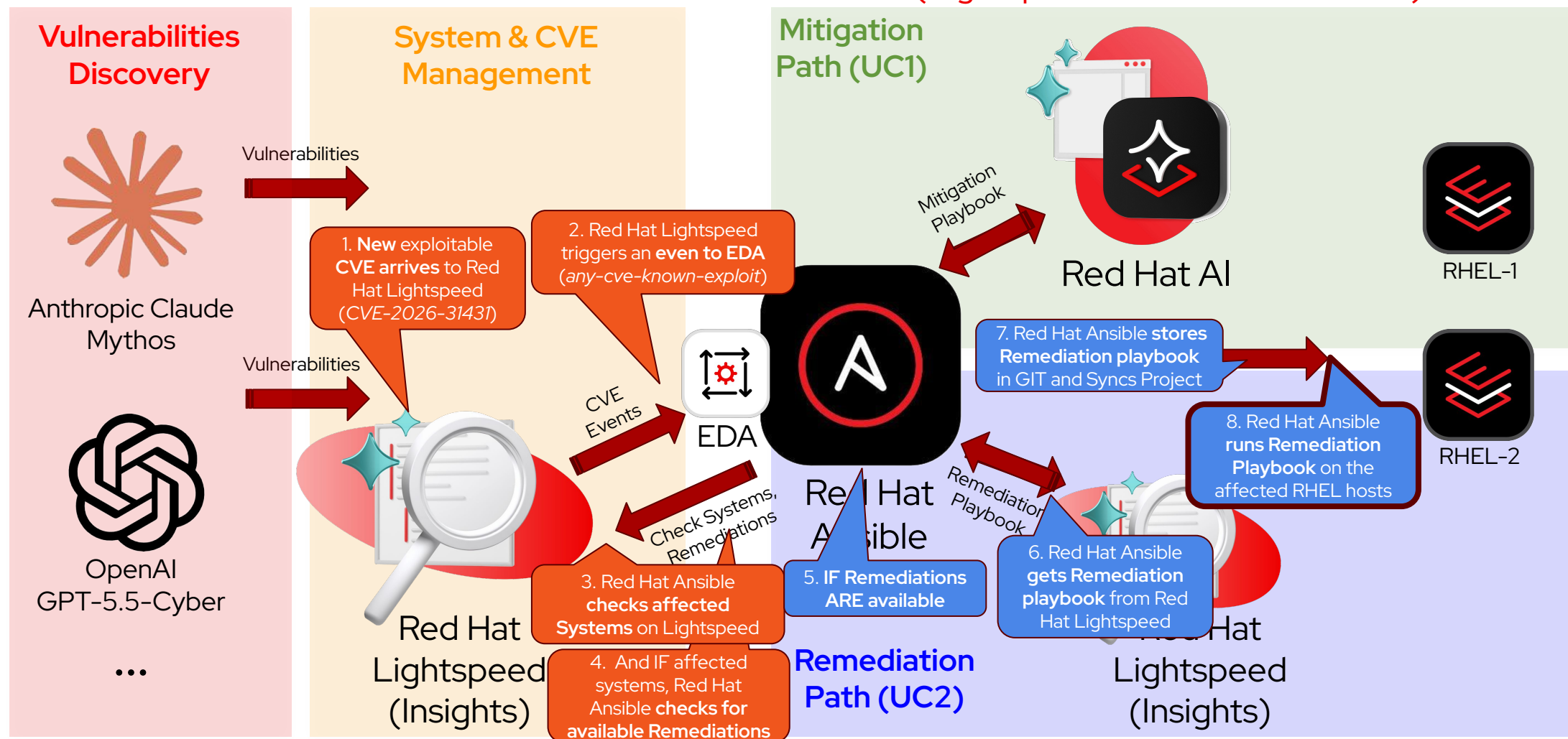


Use Case 2: New CVE arrives with Remediation (Lightspeed-based Remediation)



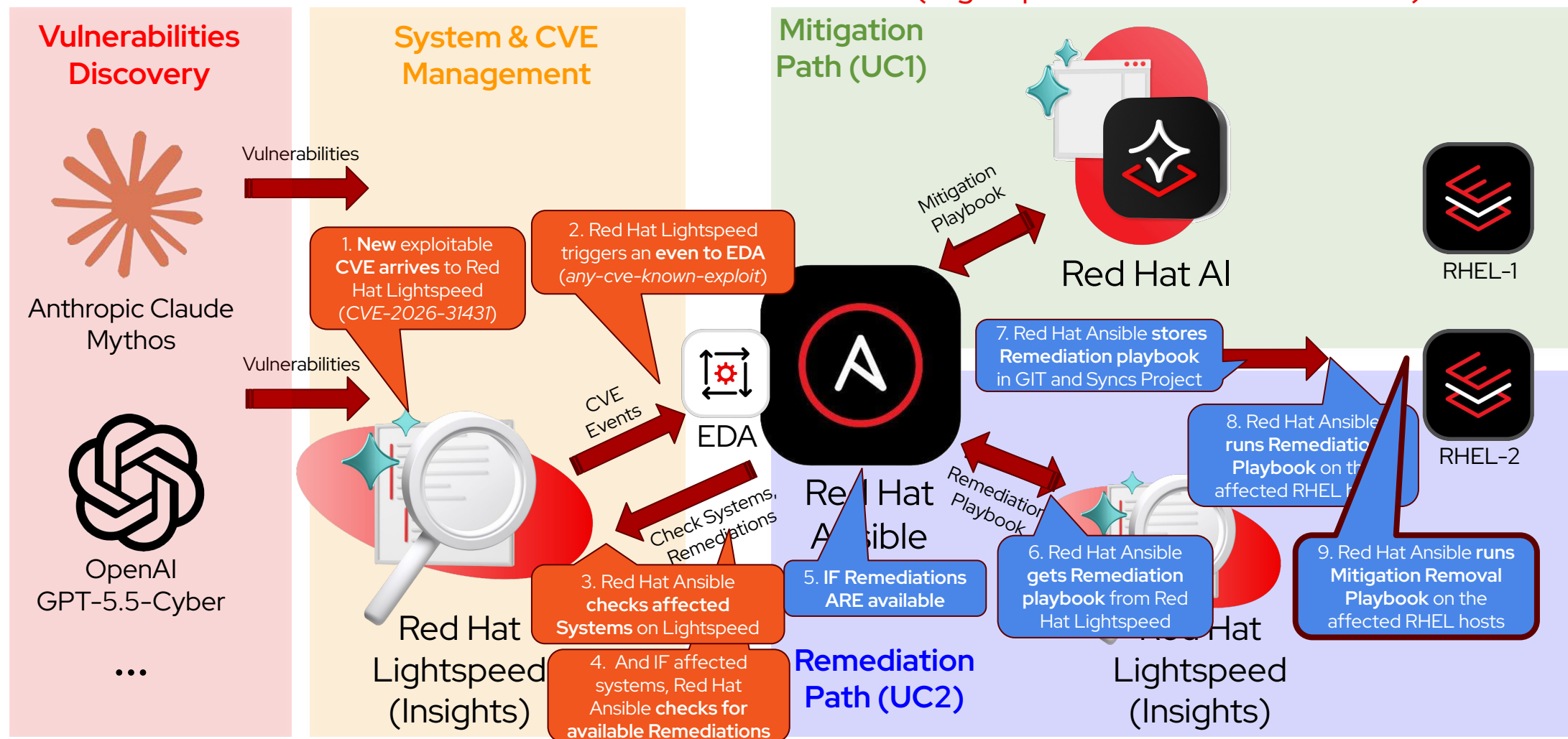
AIOps: Mitigation and Remediation of CVEs

Use Case 2: New CVE arrives with Remediation (Lightspeed-based Remediation)



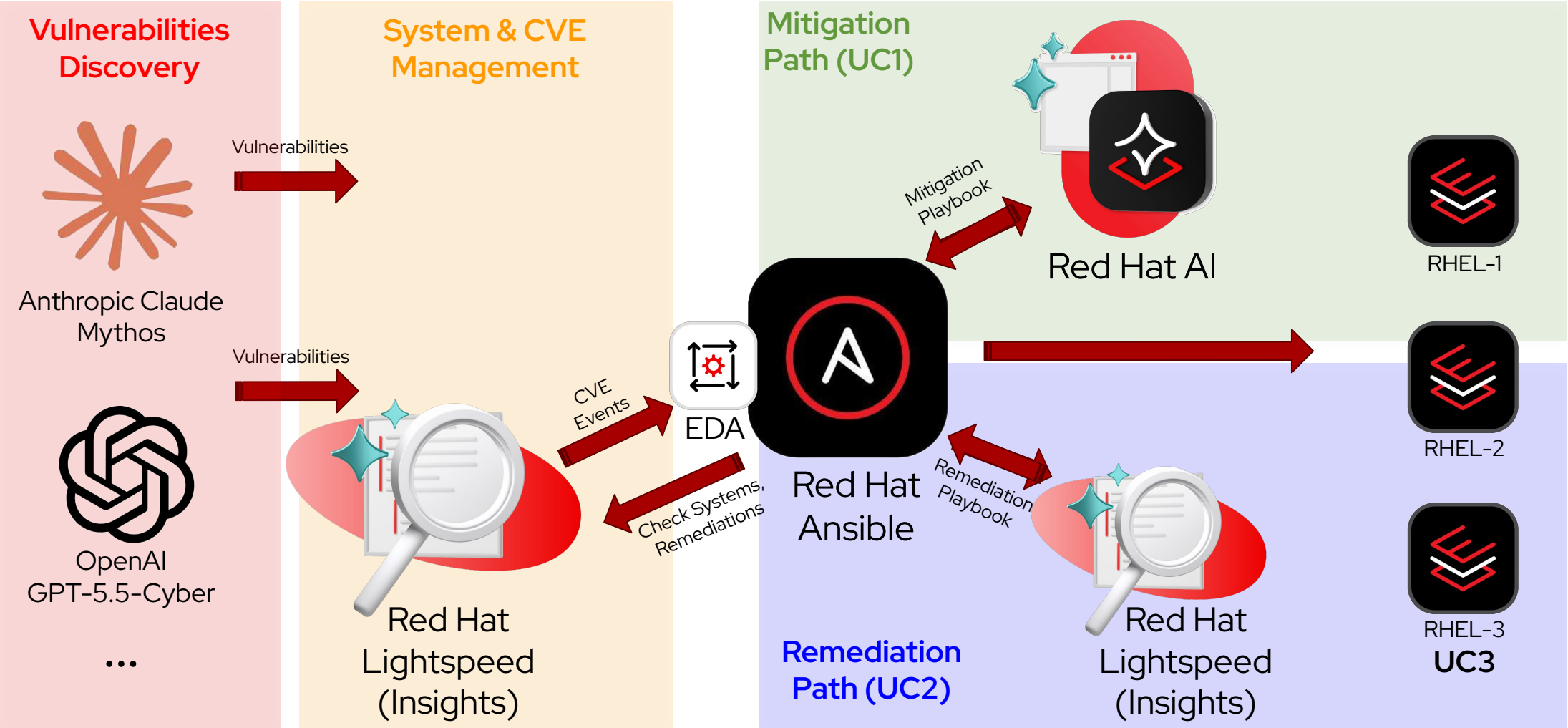
AIOps: Mitigation and Remediation of CVEs

Use Case 2: New CVE arrives with Remediation (Lightspeed-based Remediation)



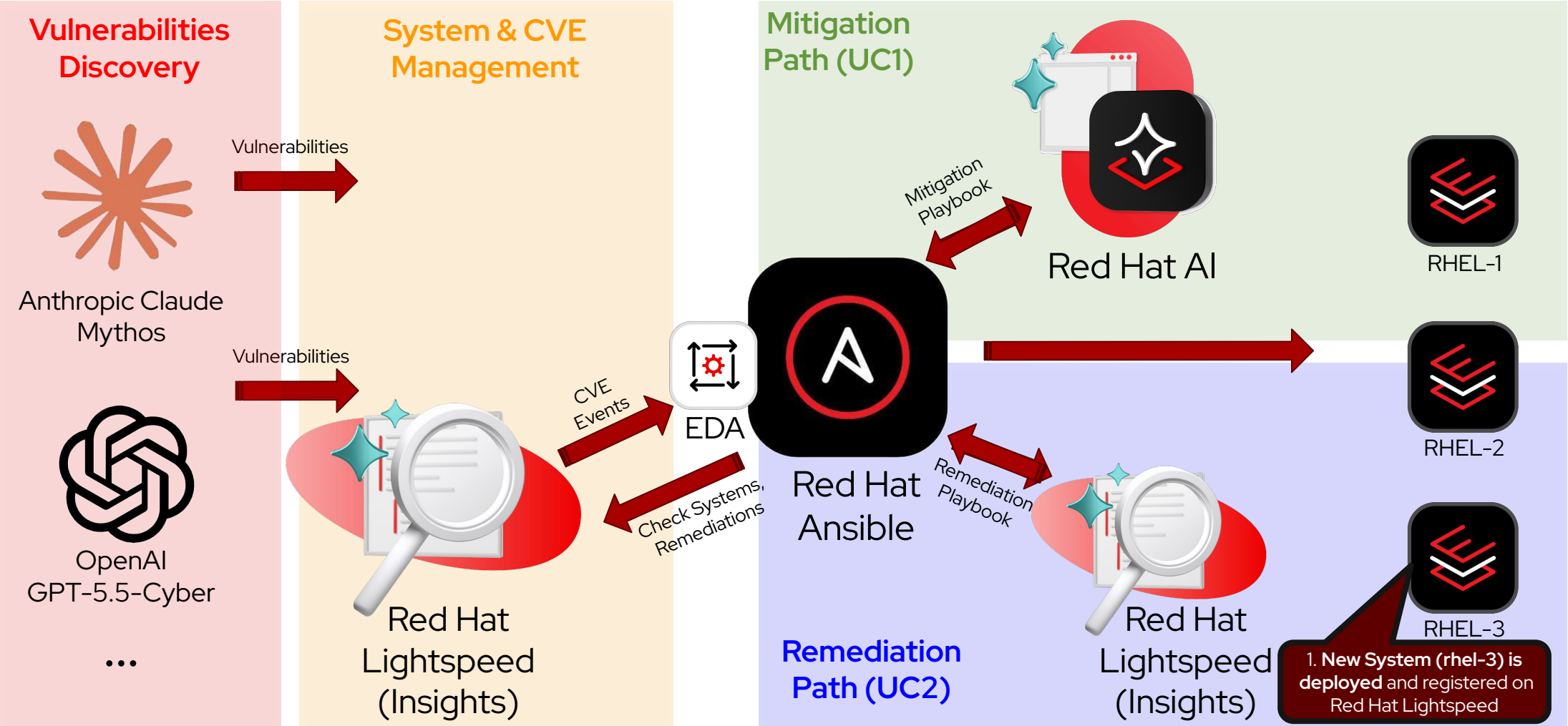
AIOps: Mitigation and Remediation of CVEs

Use Case 3: New System is deployed (Lightspeed-based Remediation and/or AI-based Mitigation)



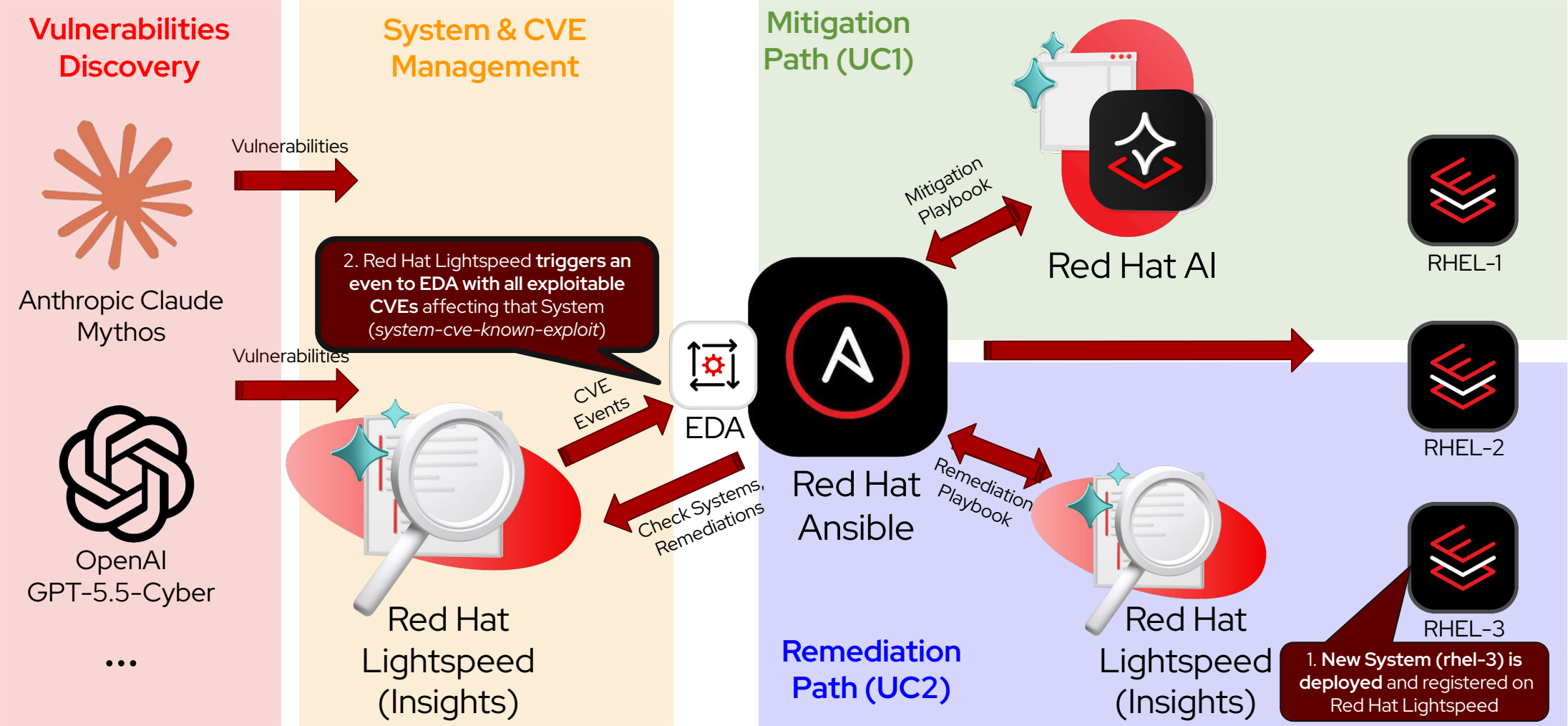
AIOps: Mitigation and Remediation of CVEs

Use Case 3: New System is deployed (Lightspeed-based Remediation and/or AI-based Mitigation)



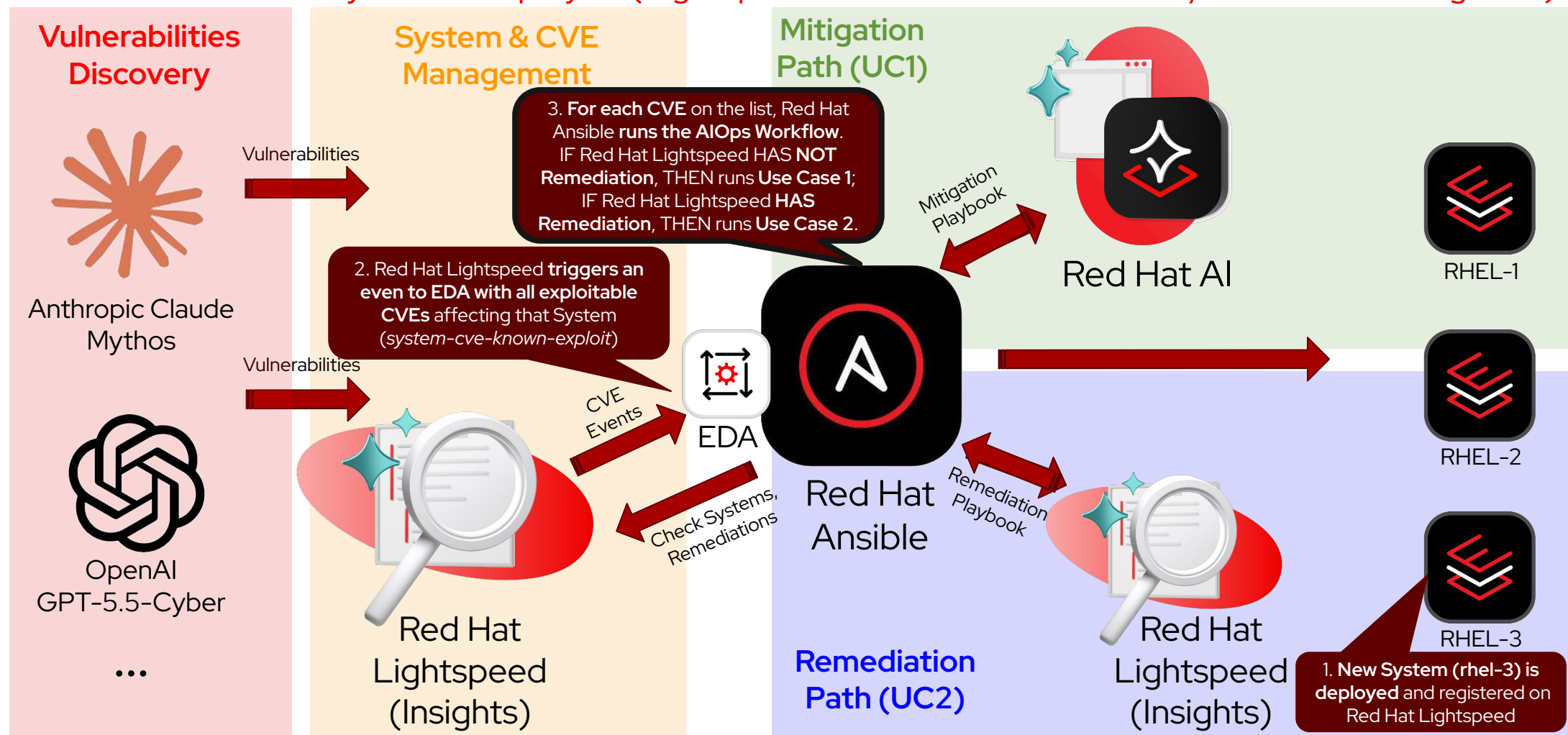
AIOps: Mitigation and Remediation of CVEs

Use Case 3: New System is deployed (Lightspeed-based Remediation and/or AI-based Mitigation)



AIOps: Mitigation and Remediation of CVEs

Use Case 3: New System is deployed (Lightspeed-based Remediation and/or AI-based Mitigation)



Demo Time!

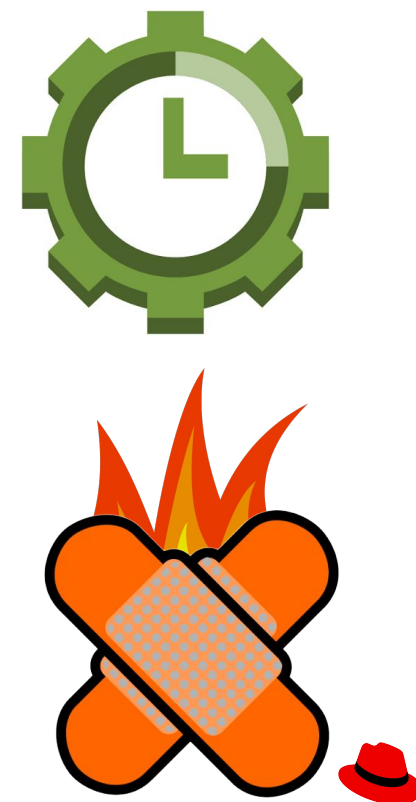


Other Demo Variantes

Similar Use Cases: RHEL and Other Domains

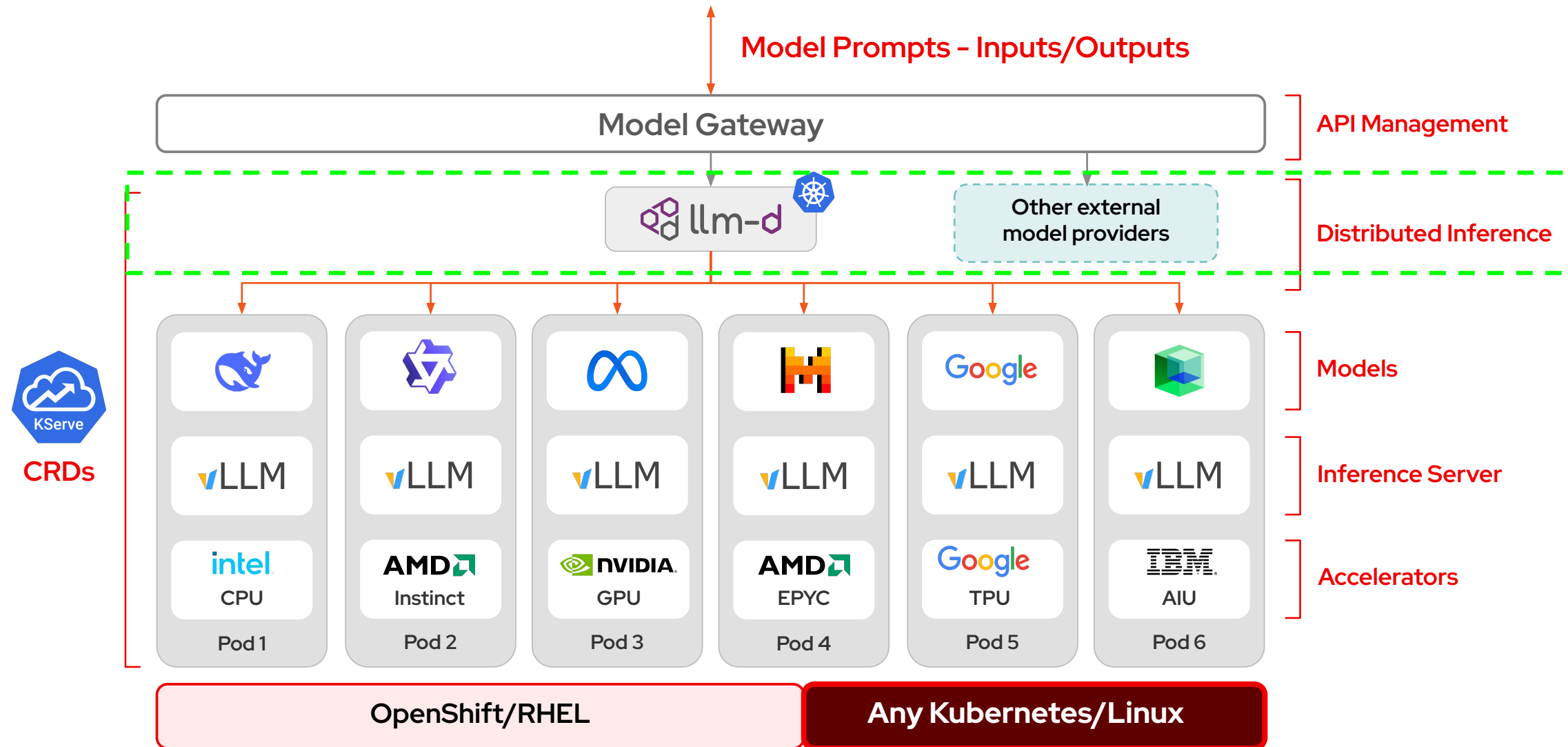
This demo showed an example to showcase the potential of the solution. However, **Use Cases variants can be implemented**, on RHEL, or other domains:

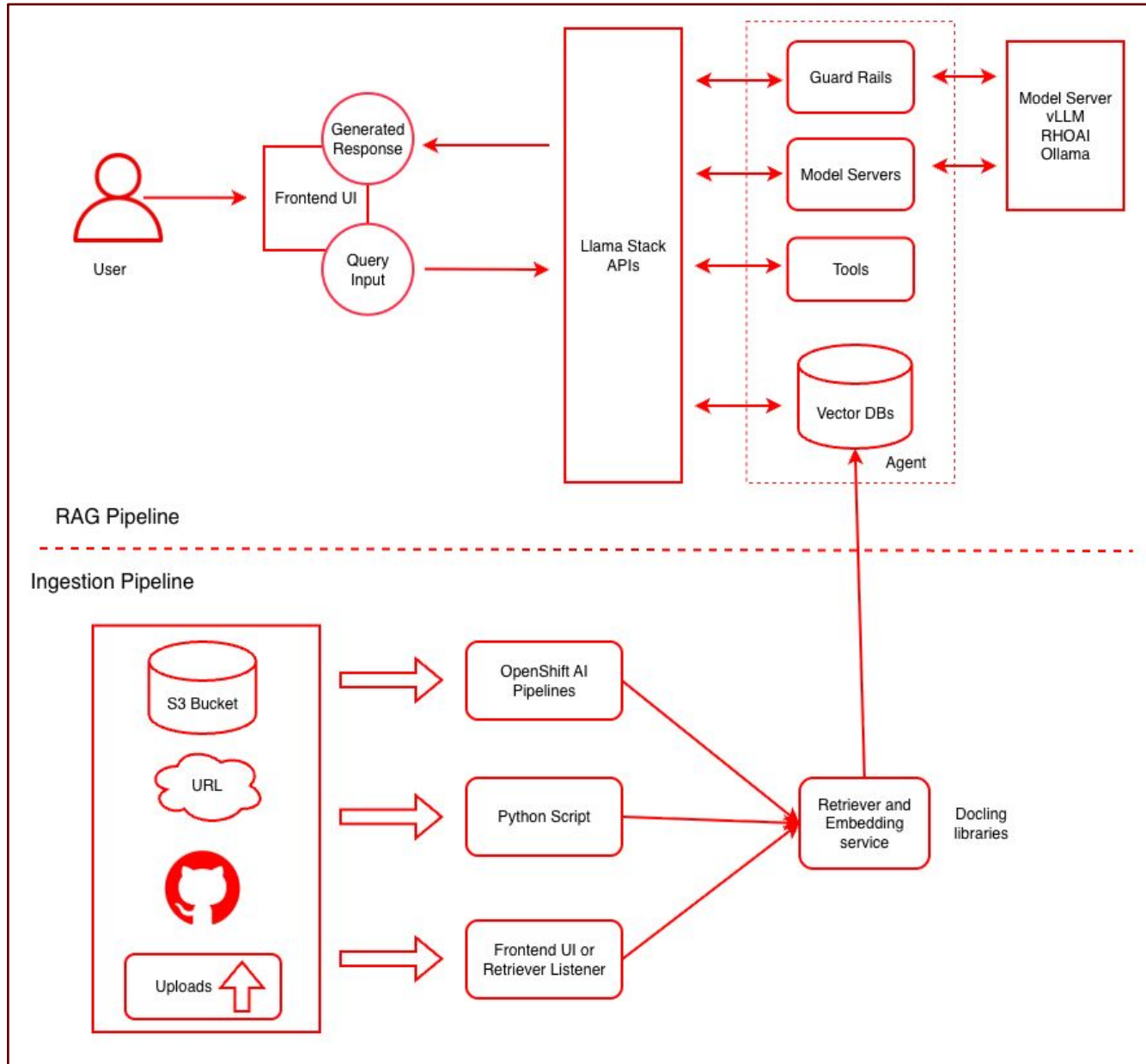
- ▶ Maintenance Windows
 - **Mitigate**, while waiting for a Maintenance Window (prod)
 - **Remediate**, when there is Maintenance Window in (prod)
- ▶ Reboot Required
 - **Mitigate**, if remediation DOES requires reboot (cold patching)
 - **Remediate**, if remediation DOES NOT require reboot (hot patching)
- ▶ Others: Extend to other CVE types, CVE sources and domains



Enterprise GenAI Inference Platform

Holistic approach to optimize and operationalize deployment and scaling of open-source LLMs





Red Hat's Stack for Real-World RAG



Securely deploy anywhere



Validated and optimized models



Fast, flexible inference with vLLM

Tech Journey demos: Red Hat Security



Webinar

Desplegando una fortaleza digital: no confíes,
siempre verifica y encripta tus datos

23 de octubre de 2026, 10:00 a.m.



Webinar

Automatización y seguridad: estrategia de
remediación integral con Red Hat

13 de noviembre de 2026, 10:00 a.m.





Hands-on Workshop Week • November 30, to December 4, 2026

Red Hat Tech Journey workshop week

One week. Four areas shaping enterprise IT. Hands-on experience.



Discover how to apply open source technologies to build secure platforms, automate operations, and run modern applications across hybrid environments.

Red Hat
Summit

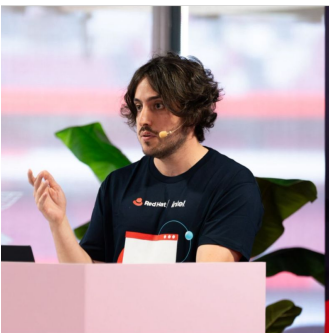
Connect

Thank you



Carlos Parada

Senior Specialist Solution Architect (*Ansible*)
Red Hat



Nelson Paez

Specialist Solution Architect (*Openshift AI*)
Red Hat

