

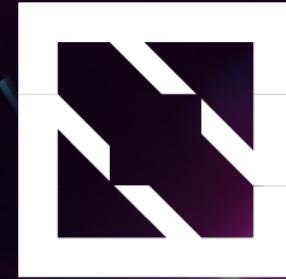


KubeCon

THE LINUX FOUNDATION



China 2024



CloudNativeCon





KubeCon



CloudNativeCon



China 2024

Enhancing Cyber Resilience

Through Zero Trust Chaos Experiments in Cloud Native Environments

Rafik Harabi, Senior Solutions Architect - Sysdig
Sayan Mondal, Senior Software Engineer - Harness

Who we are?



KubeCon



CloudNativeCon



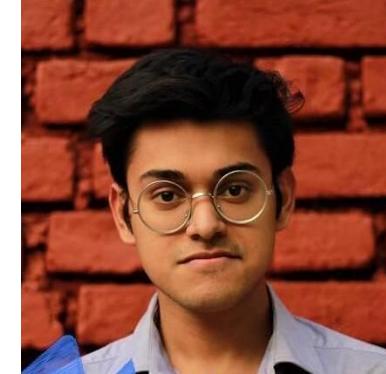
THE LINUX FOUNDATION
OPEN SOURCE SUMMIT



China 2024



- Senior Solution Architect at Sysdig, Cloud Security Advocate
- Focus on Cloud Native Security
- Previously working on go to Cloud programmes



- Senior Software Engineer II at Harness
- Maintainer of LitmusChaos (CNCF Incubating)
- LFX Mentor
- Chaos Engineering Practitioner



[rafikharabi](#)



[@rafik8_](#)



[s-ayanide](#)



[@s_ayanide](#)

Agenda

- Cloud Native Application and Threat Landscape
 - Chaos Engineering and Cyber Resilience
 - Enhance Security with Chaos Engineering
 - Solutions Architecture
 - Tooling and Architecture
-
- Hands on demo
 - Next steps
 - Takeaways

Once, there was a perimeter

You had a perimeter **guarded
by a firewall**

Detecting intrusions was
your breach indicator



KubeCon



CloudNativeCon



China 2024



Now, there is no perimeter in the cloud



KubeCon



CloudNativeCon



China 2024



Cloud providers own external connections



Cloud is exposed to the outside world



You need to control access to services your team uses



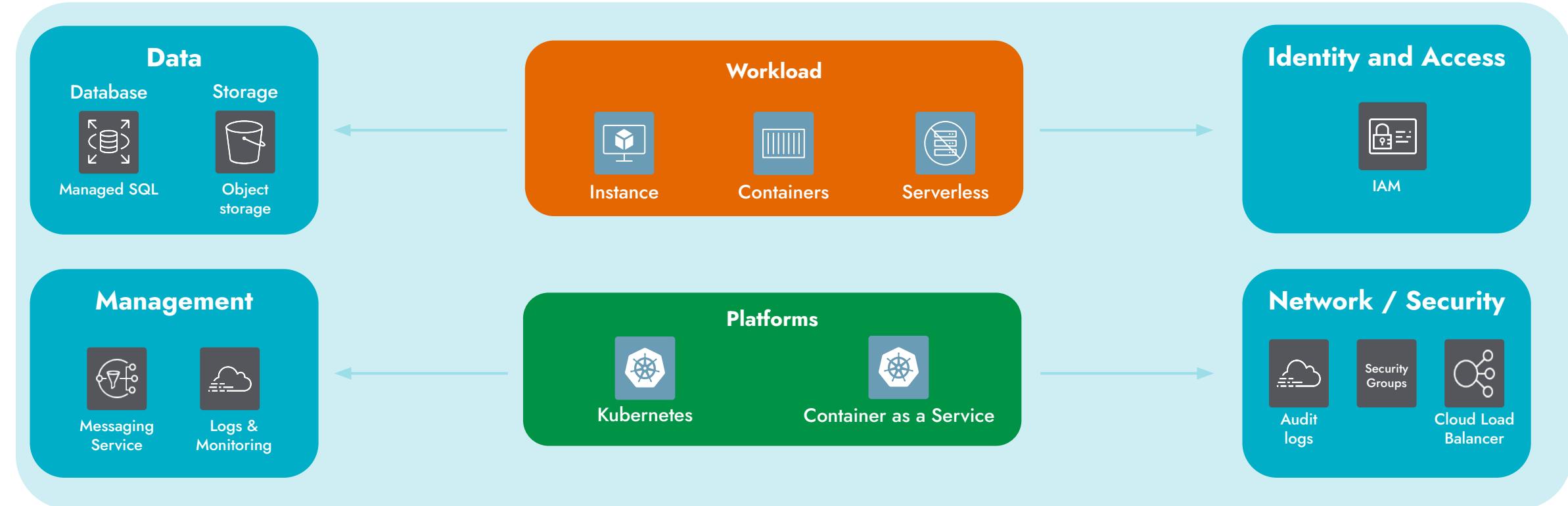
You need to detect unusual activity



Cloud Native Application Architecture



China 2024



Cloud Provider



Cloud Application Security Challenges

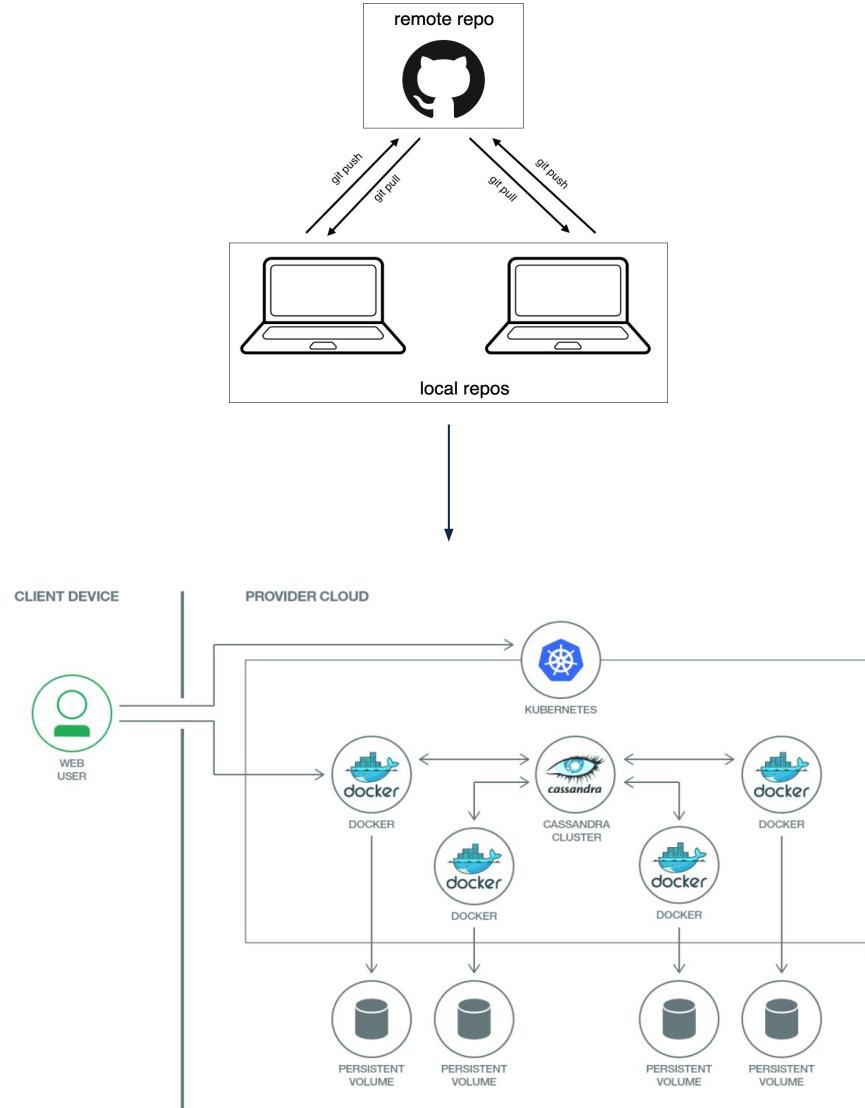


- Dynamic attack surface,
- Threat actors are using your tools today,
- Distributed systems and microservices enlarge attack surface,
- Number of calls generated by distributed systems,
- Lack of visibility,
- Cloud delivery vs security process speed.

Manufacturing software in Cloud Native era



China 2024

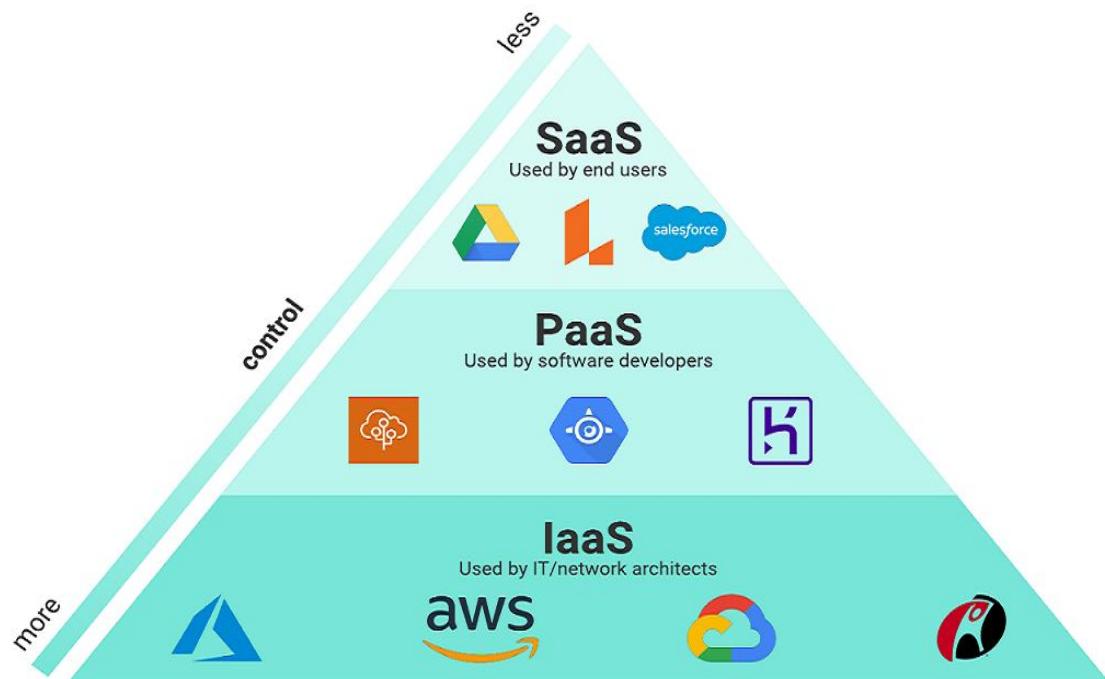


- Runtime architecture, CI/CD, DevOps, Environments, SecOps, Configuration Management, Version Management, Testing, Observability, Analytics, SRE
- Devops goes to canary, etc
- Self Service and Policy Driven
- Zero Trust environment

The *Cloud Native* problem

Microservices proliferation leads to a RELIABILITY challenge

Cloud-native code's reliance on numerous microservices and platforms heightens failure risks.



Legacy DevOps



Cloud-Native DevOps



What causes Downtime?



KubeCon



CloudNativeCon



THE LINUX FOUNDATION
OPEN SOURCE SUMMIT



AI_dev
Open Source Dev & ML Summit

China 2024

Application Failures

- Excessive Logging to debug
- Too many retries
- Service Timeout

Infrastructure Failures

- Device failures
- Network failures
- Region not available

Operational Failures

- Capacity issues
- Incident management
- Monitoring dashboards not available

Reputational Impact

 Slack Status @SlackStatus · Mar 9
We've resolved the issue, but please note some features may take a bit longer for the fix to take effect. You may need to reload Slack (Cmd/Ctrl + Shift + R) to see the fix on your end. Apologies for the disruption!

Slack's Outages

Financial Impact

 Wells Fargo @WellsFargo · Feb 7, 2019
We want our customers to know that this is a contained issue affecting one of our facilities, and not due to any cybersecurity event. We apologize for the inconvenience caused by these system issues, and any Wells Fargo fees incurred as a result of these issues will be reversed.

Est. >\$55M in losses to WF

Poor User Experience

 British Airways @British_Airways
Replying to @JPipDavis
I'm afraid we're currently experiencing some system issues at the airport this morning, Pip. We're doing all we can to resolve this and 1/2

75,000+ passengers travel plans impacted



Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

20% complete



For more information about this issue and possible fixes, visit <https://www.windows.com/stopcode>

If you call a support person, give them this info:

Stop code: CRITICAL_PROCESS_DIED

Bad Actors Exploiting Vulnerabilities



KubeCon



CloudNativeCon



China 2024



What is Chaos Engineering?



KubeCon



CloudNativeCon



China 2024



“

Chaos engineering is the process of testing a distributed computing system to ensure that it can withstand unexpected disruptions.

—
Tech Target
(<https://www.techtarget.com>)

What is Cyber Resilience?



KubeCon



CloudNativeCon



China 2024



“

Security Chaos Engineering (SCE) is a novel approach to cyber security; its core fundamentals are based on the principles of chaos engineering, though the objective is to enable cyber resiliency.

—
Mitigant
(mitigant.io)

Red Team strategies



KubeCon



CloudNativeCon



THE LINUX FOUNDATION
OPEN SOURCE SUMMIT



China 2024

Pen Testing

- focus on a specific asset and have a defined scope that restricts the penetration tester.
- conducted periodically.

Adversary Emulation

- Emulating specific threat actors/attack scenarios.
- focusing on specific attack vectors and techniques used by particular adversaries.

Security Chaos Eng

- Introducing controlled security failures.
- observe how the system responds and recovers.
- Ongoing practice

Why Security Chaos Engineering ?

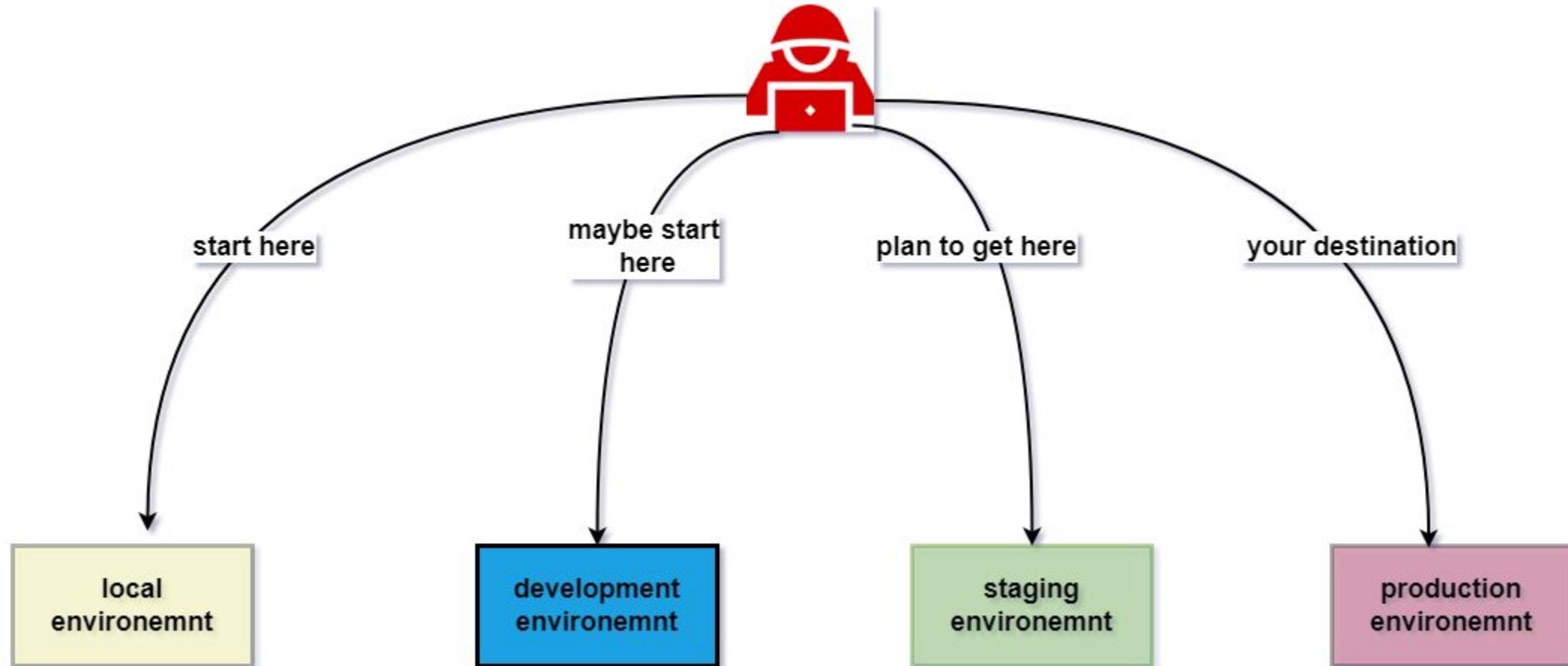


China 2024

Security Chaos Engineering complements traditional security practices :

- Proactive approach,
- Integrated into ongoing security practices,
- Providing continuous feedback and improvement.

Where to practise this?



Is Reliability a goal in Security?

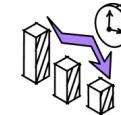


China 2024

It is not a direct goal usually, but Reliability of the end product or service is being affected while solving the other challenges.



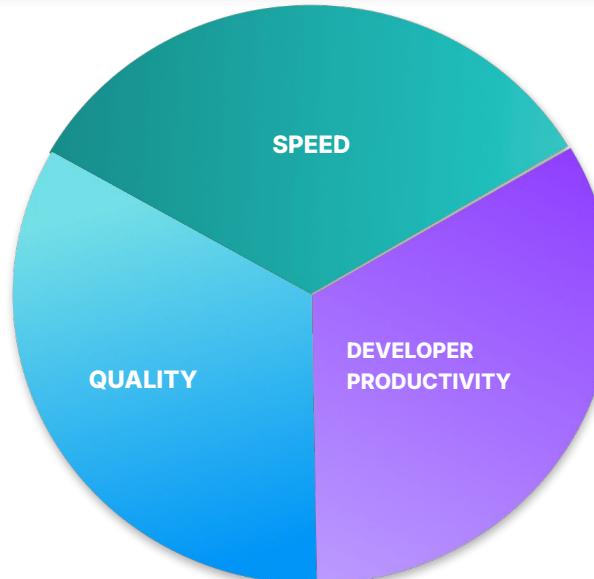
Are you sure you are not compromising the reliability?



How much of developer time is being spent on issues related to reliability?



Have you verified that the known resilience status is intact? No new bugs being leaked into the product?



The Chaos Engineering Process



KubeCon



CloudNativeCon



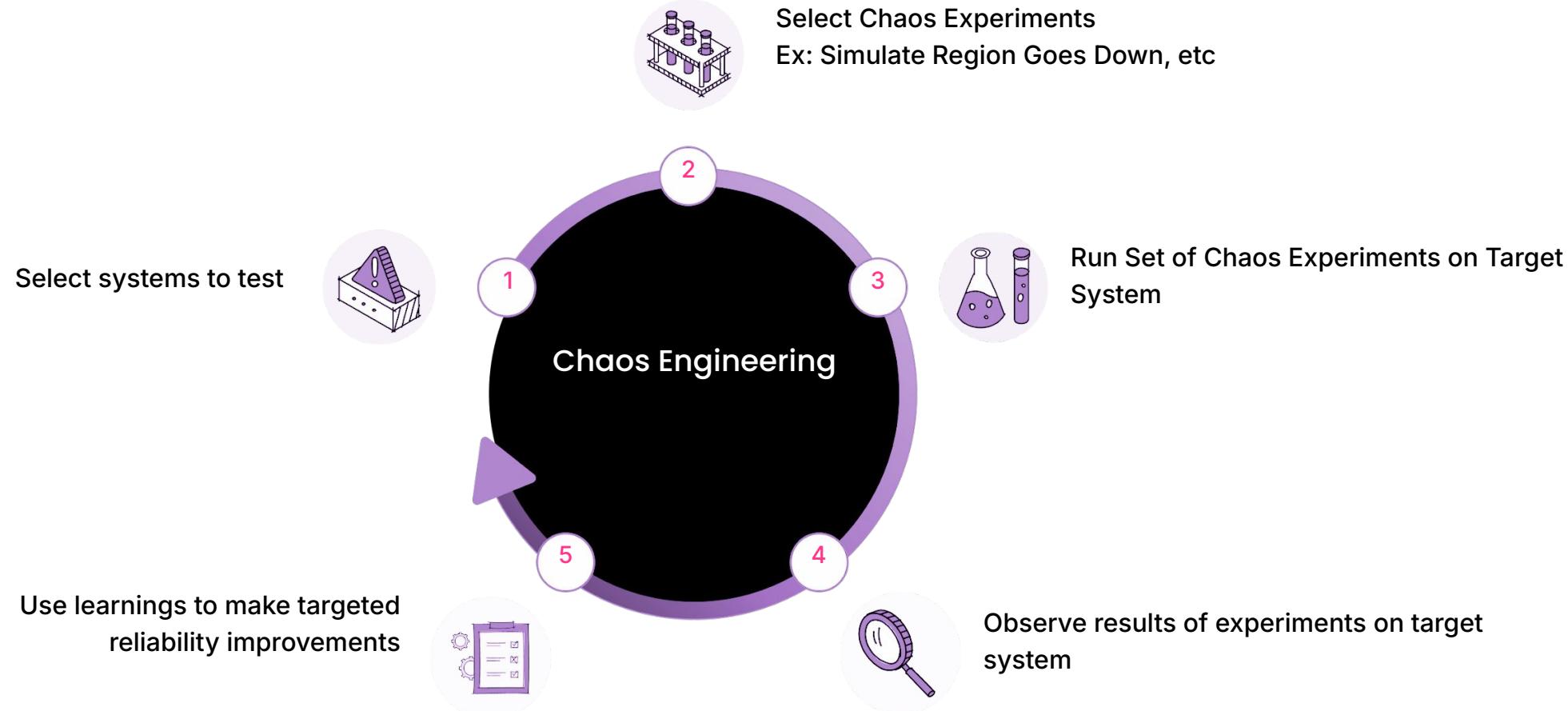
THE LINUX FOUNDATION

OPEN SOURCE
SUMMIT



AI_dev
Open Source Dev & ML Summit

China 2024



The Problems in current solutions



KubeCon



CloudNativeCon



China 2024



Existing solutions



Failures impacting resiliency is inevitable

- Not proactively managed
- Downtimes maybe expensive



Failure Scenarios are Difficult to Implement

- Isn't implemented in a safe/controlled environment
- Isn't collaborative
- Not scalable



Failure Testing isn't automated

- Believed to be just for Ops
- Difficult to manage chaos in CI/CD
- No monitoring of impact

A Better Solution



KubeCon



CloudNativeCon



OPEN
SOURCE
SUMMIT



China 2024

Chaos engineering is *collaborative*



Collaborative chaos experiments in a centralized control plane

SREs + Developers

Experiments are in Git just like code

Robust Experiments



Public and private chaos hubs with ready to use experiments

Optimize initial investment

Reduce the inertia for starting chaos

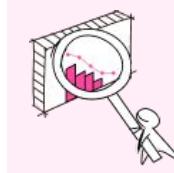
Integrate into CI/CD systems



Rollout automated and controlled chaos experiments across prod/non-prod environments

Find weaknesses during build/test phase

Verifying at dev stage saves money



Enables observability for Chaos

Chaos metrics used to assess impact and manage SLOs/Errors

Measure the impact of inducing chaos

Build confidence by starting small

Is it really a better solution?



KubeCon



CloudNativeCon



THE LINUX FOUNDATION

OPEN SOURCE SUMMIT



Open Source Dev & ML Summit

China 2024

Gaining Kernel Level Visibility



Kernel-level visibility helps detecting sophisticated threats that traditional security approaches might miss

Comprehensive Security Coverage



Ensures comprehensive security coverage addresses potential blind spots in the current chaos engineering framework.

Real Time Threat Detection



Enables faster response to potential security incidents.

Customisable Rules and Policies



Flexibility in creating customizable rules and policies tailored to specific security needs and threat models.

Potential Tools



Litmus Chaos is an Open Source Cloud-Native Chaos Engineering Framework with cross-cloud support. It is a CNCF Incubating project with adoption across several organizations.

<https://litmuschaos.io>



Falco is a cloud-native security tool designed for Linux systems. It employs custom rules on kernel events, which are enriched with container and Kubernetes metadata, to provide real-time alerts

<https://falco.org>



KubeCon



CloudNativeCon



THE LINUX FOUNDATION
OPEN SOURCE SUMMIT

China 2024

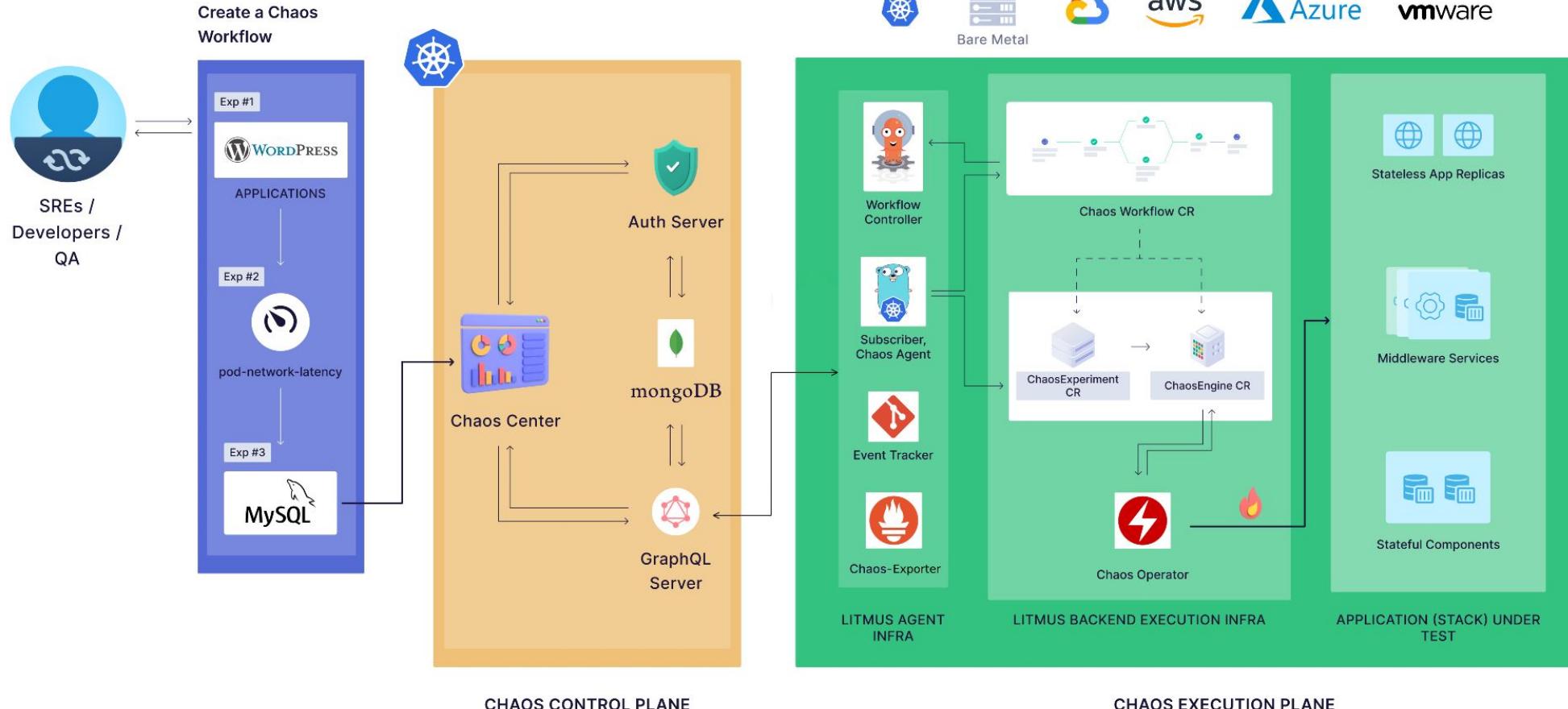


AI_dev
Open Source Dev & ML Summit

How does Litmus work?



China 2024



How does Litmus work?



KubeCon



CloudNativeCon



China 2024



Chaos Operator

Chaos CRDs



Threat Detection with Falco



KubeCon



CloudNativeCon



THE LINUX FOUNDATION
OPEN SOURCE SUMMIT



AI_dev
Open Source DevOps & ML Summit

China 2024

Falco is an **open source** runtime security solution for **threat detection** across **Kubernetes**, containers, hosts and **the cloud**.

CNCF Graduated Project
(Feb. 2024)



★ 7.2k

 50M+ pulls

<https://falco.org>

<https://github.com/falcosecurity/falco>

Falco Architecture Overview



KubeCon



CloudNativeCon

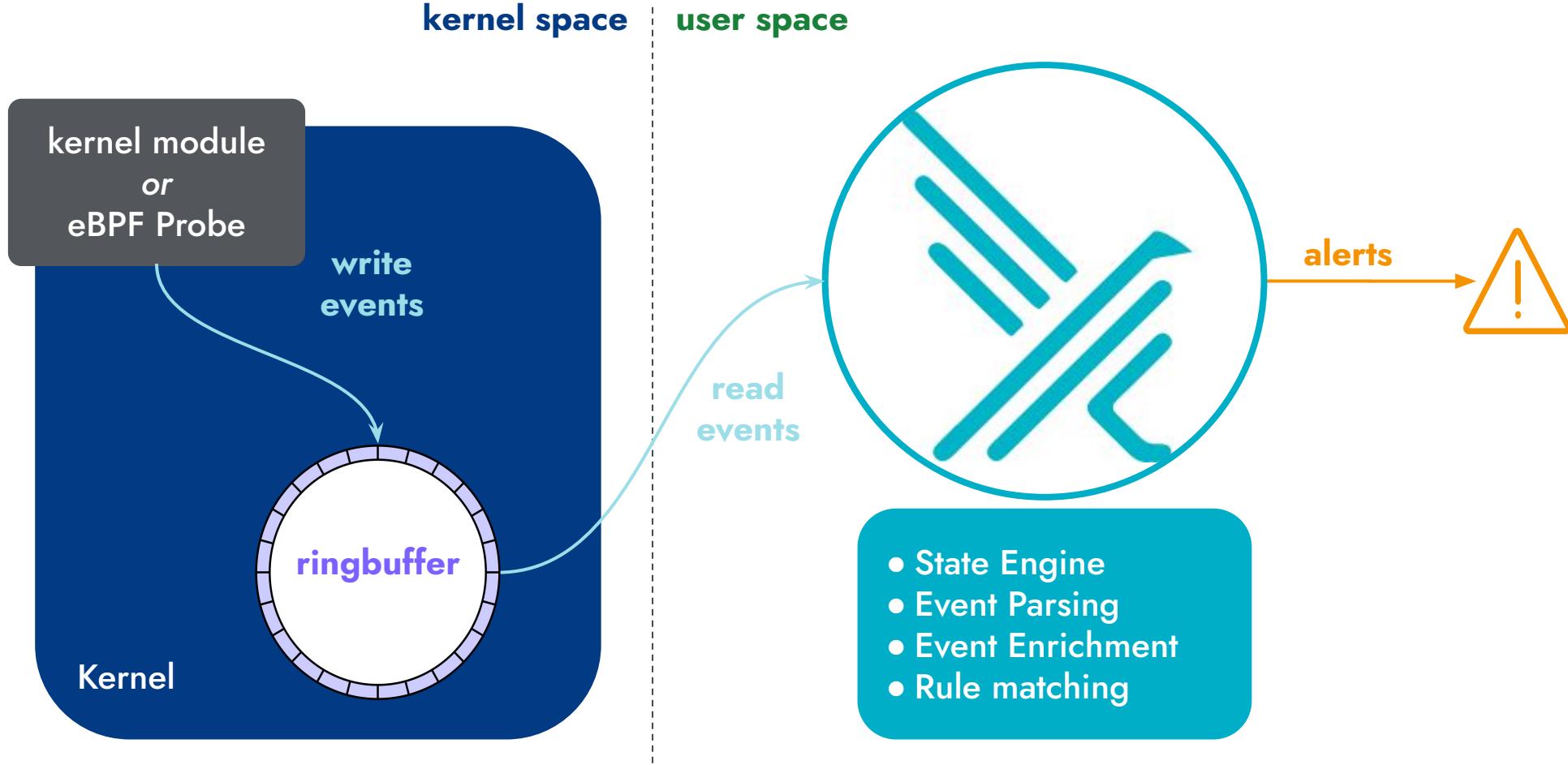


THE LINUX FOUNDATION
OPEN SOURCE SUMMIT



AI_dev
Open Source Dev & ML Summit

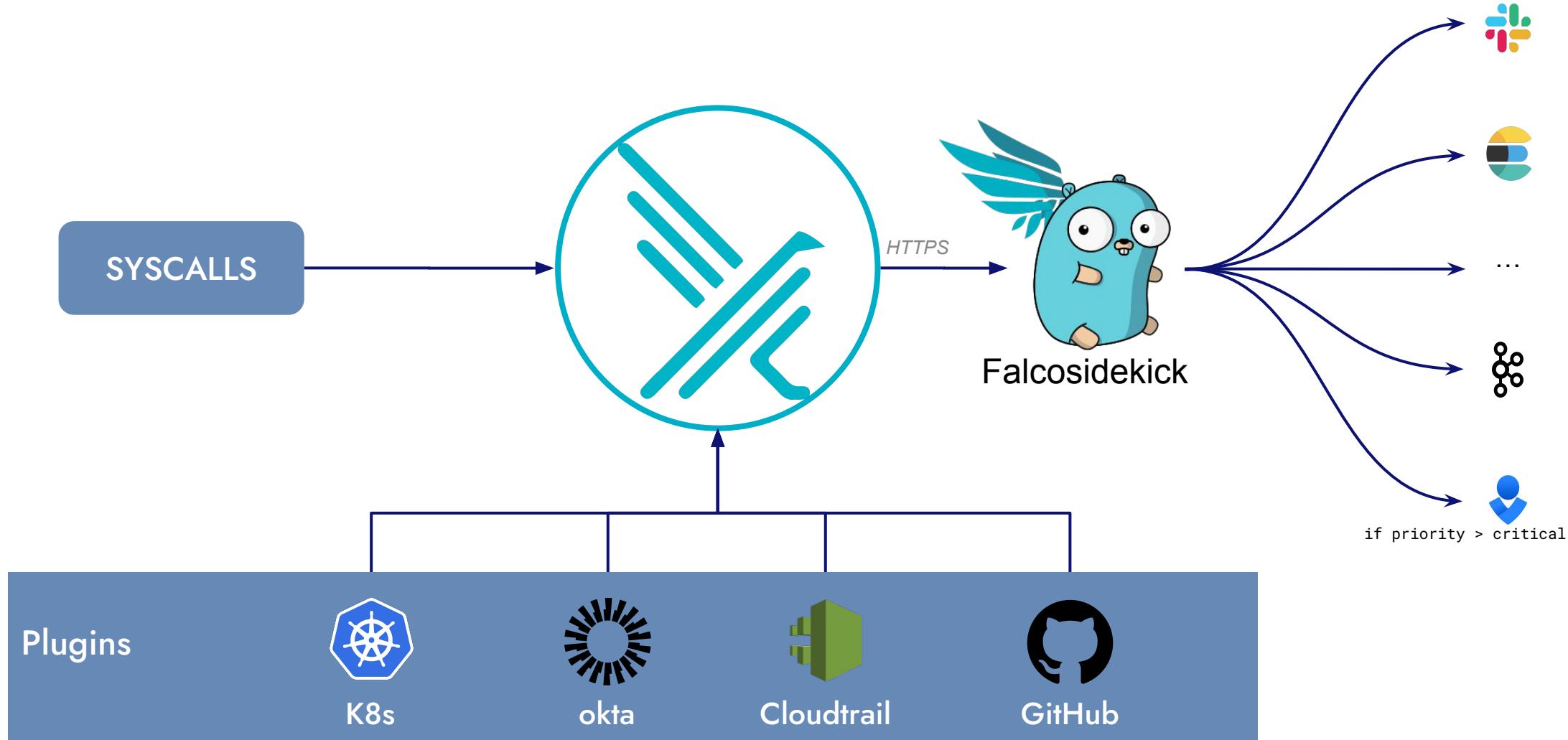
China 2024



Falco Ecosystem



China 2024



Hands on Demo

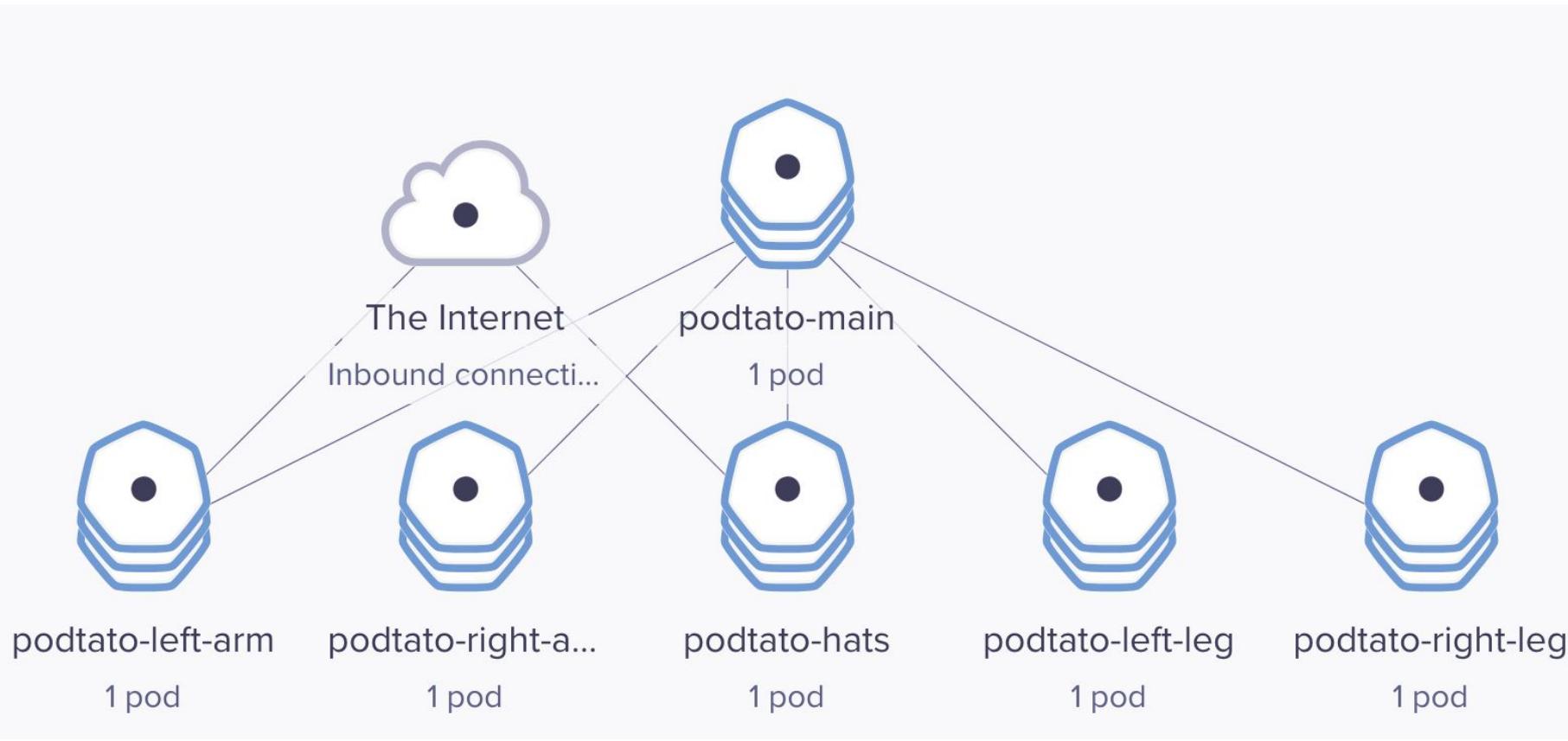
<https://github.com/S-ayanide/kubecon-china-2024-cyber-resilience-falco-litmuschaos>

<https://tinyurl.com/kubecon-china-24>

Podtato Demo Application



China 2024

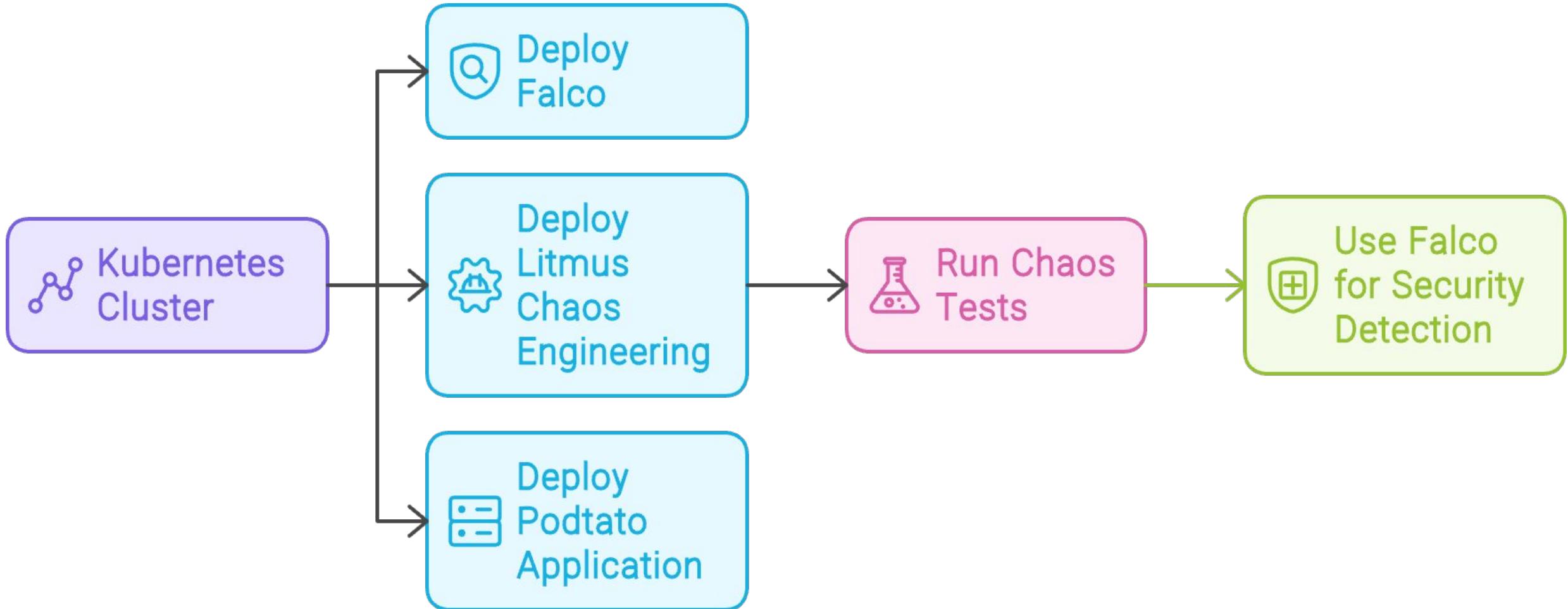


<https://github.com/podtato-head/podtato-head/tree/main>

Chaos Engineering in practice



China 2024

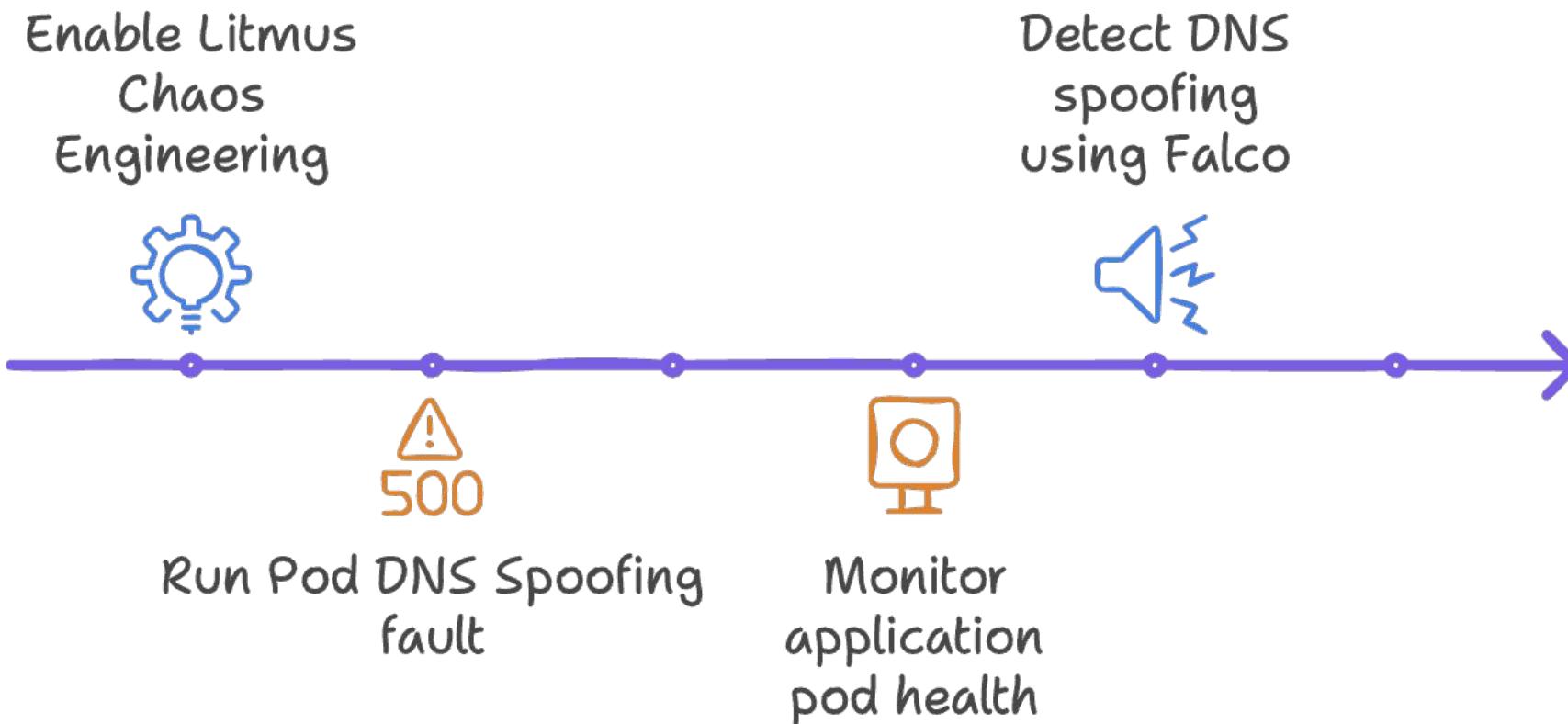


Scenario 2 - DNS spoofing



China 2024

Run Litmus Chaos Engineering to perform DNS spoofing of Kubernetes Pods



Scenario 2 - Falco Detection Rule



KubeCon



CloudNativeCon



THE LINUX FOUNDATION

OPEN SOURCE SUMMIT



Open Source Dev & ML Summit

China 2024



```
- rule: Detect Access to resolv.conf by Root User
  desc: Detect access to /etc/resolv.conf only when performed by root user
  condition: >
    container and
    fd.name = /etc/resolv.conf and
    user.name = "root"
  output: "[KubeCon] Access to /etc/resolv.conf detected by root user (container=%container.name
user=%user.name command=%proc.cmdline)"
  priority: WARNING
  tags: [filesystem, container]
```

Scenario 2 - Video Demo



KubeCon



CloudNativeCon



THE LINUX FOUNDATION
OPEN SOURCE SUMMIT



AI_dev
Open Source Dev & ML Summit

China 2024

The screenshot shows the Litmus 3.0 Experiment Builder interface. On the left, a sidebar menu includes 'Overview', 'Chaos Experiments' (which is selected and highlighted in purple), 'Environments', 'Resiliency Probes', 'ChaosJobs', and 'PROJECT SETUP'. The main workspace displays a 'dns-spoof' experiment under 'My Project > Chaos Experiments'. The 'Experiment Builder' tab is active, showing a network diagram with two nodes: 'pod-dns-spoof-p01' and 'pod-dns-error-kub'. A connection line between them has a small '+' icon at its midpoint, indicating it can be modified or added to. The top right of the workspace features buttons for 'CREATE STATUS', 'Run History', 'Unsaved Changes', 'Save', 'Share', and 'Run'. Below the workspace, there are sections for 'Overview', 'Experiment Builder', and 'Schedule'. The bottom right corner contains a vertical toolbar with icons for 'New', 'Edit', 'Delete', and 'Import'.

Scenario 1 - Modify HTTP header



KubeCon



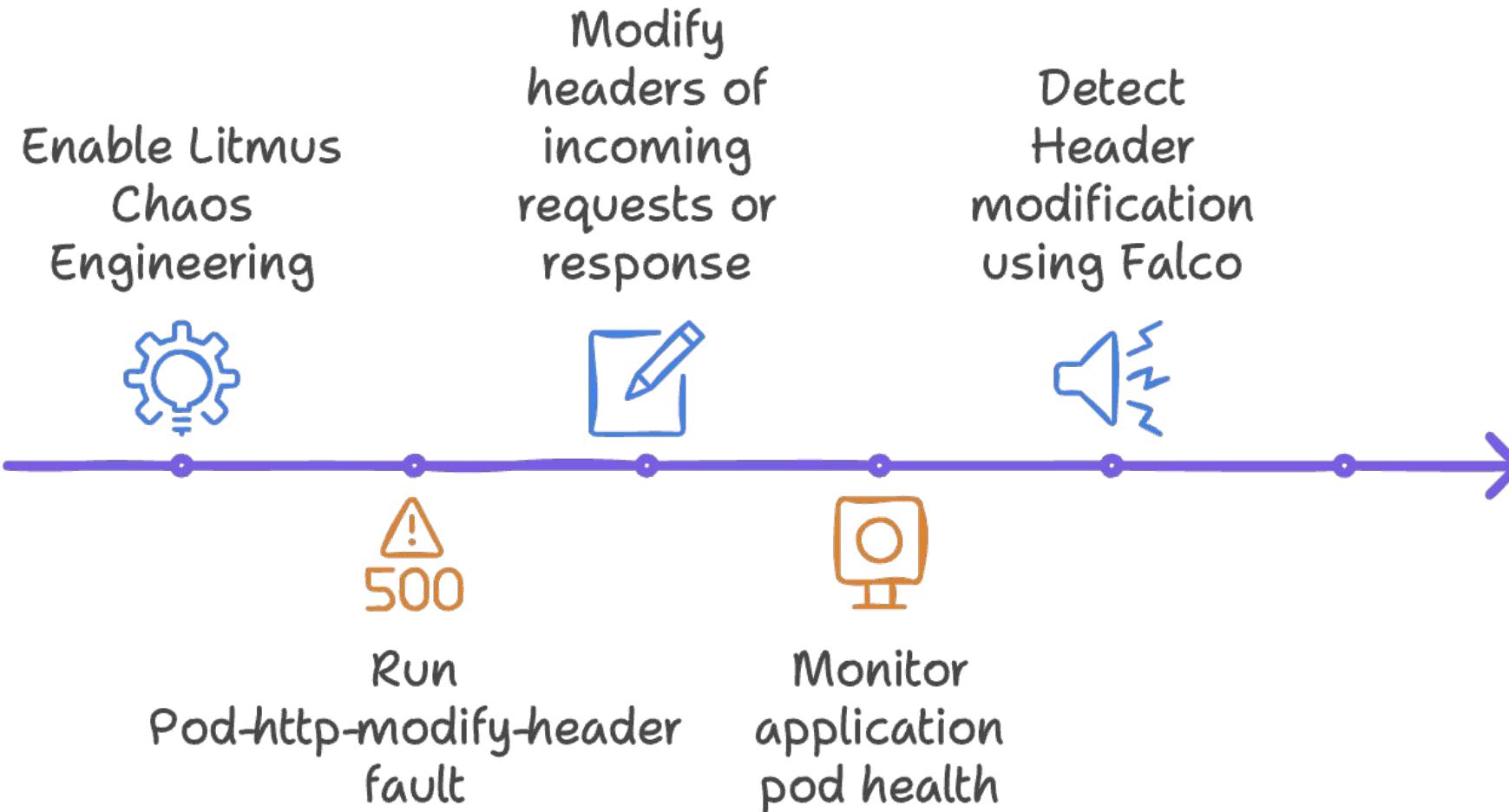
CloudNativeCon



China 2024



Run Litmus Chaos Engineering to Modify HTTP Headers of Kubernetes Pods



Scenario 1 - Falco Detection Rule



China 2024



```
- rule: Detect Header Detection in Log File
  desc: Detects when the specific text "Header X-Litmus-Test-Header detected" is logged
  condition: >
    container and
    fd.name = /tmp/http_header_check.log and
    evt.type in (open, read, write) and
    (proc.cmdline contains "cat" or proc.cmdline contains "grep" or proc.cmdline contains "tail")
  output: "[KubeCon] [HTTP Headers Modify] Detected log entry indicating HTTP header detection
(container=%container.name user=%user.name command=%proc.cmdline file=%fd.name)"
  priority: WARNING
  tags: [filesystem, http]
```

Scenario 1 - Video Demo



KubeCon



CloudNativeCon



THE LINUX FOUNDATION
OPEN SOURCE SUMMIT



AI_dev
Open Source Dev & ML Summit

China 2024

The screenshot shows the Litmus 3.0 interface for creating a chaos experiment. On the left, a sidebar displays project navigation (Spaces, Tabs, Archive, Extensions, Window, Help) and project details (Project: admin-project, Overview, Chaos Experiments, Environments, Resilience Probes, ChaosHubs). A 'PROJECT SETUP' dropdown is also present.

The main area is titled 'My Project > Chaos Experiments > http-modify'. It features a 'CHAOSS STUDIO' header with tabs for 'VISUAL' (selected) and 'YAML'. Below this, there are buttons for 'Save', 'Discard', and 'Run'.

The central workspace displays a visual flowchart for the 'http-modify' experiment. The flow starts with a green play button icon, followed by two 'pod-http-modify-head...' components, another green play button icon, and ends with a black square icon. A dashed box labeled 'Add' is positioned between the second and third nodes. A '+' sign is located below the flowchart, and a 'Preview' and 'Advanced Options' button is visible above the flowchart.

On the right side, there are several actions: 'Clone', 'Download Manifest', and a vertical toolbar with icons for 'Edit', 'Delete', 'Add', and 'Remove'.

At the bottom left, the 'Litmus 3.0' logo is displayed, along with an 'ADMIN' icon.

Go to the next level



KubeCon



CloudNativeCon



China 2024



- Red Teaming
- Cross functional collaboration
- Enhance Automation using GitOps
- Introduce feedback loop
- Advanced Metrics
- Community and ecosystem shift

Takeaway



KubeCon



CloudNativeCon



China 2024



- Cloud-native systems exceed traditional security.
- Cyber-criminals exploit advancements in cloud.
- Learned about Zero Trust Chaos.
- Discovered vulnerabilities with chaos experiments.
- Enhanced detection and response capabilities.
- Gained actionable Zero Trust strategies.

Further Reading



KubeCon



CloudNativeCon



China 2024



- Increased support for chaos against Non-Kubernetes infrastructure components
- More Application specific chaos experiments with native faults and health checks
- Improved Chaos SDK for creation of user-defined experiments
- Additional probe types for diverse steady state-hypothesis validation
- Improved Observability for chaos experiments
- More community supported Chaos Types
- Falco training: <https://falco.org/training>
- Litmus training: <https://v2-docs.litmuschaos.io/tutorials>



KubeCon



CloudNativeCon



China 2024

Thank You

Scan QR for Feedback

Contact Sayan on

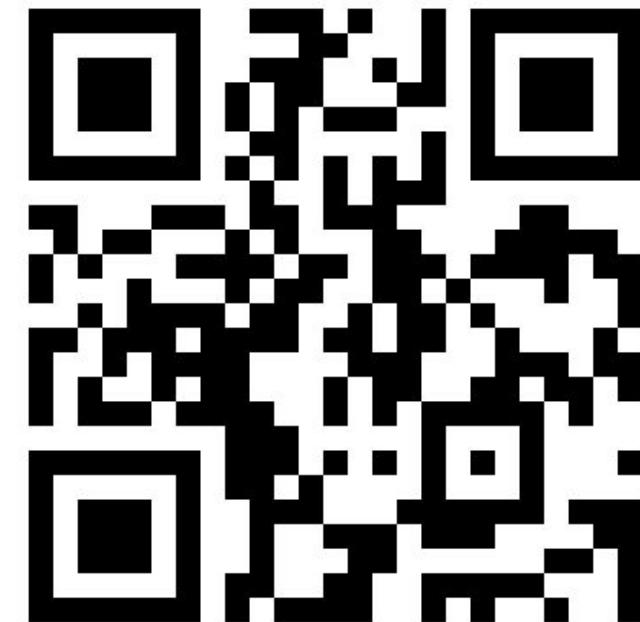


/s-ayanide

Contact Rafik on



/rafikharabi



Leave us a feedback