

BUTTERFLY EFFECT

WHAT KUBERNETES SIG SECURITY HAS IN FLIGHT

Carol Valencia

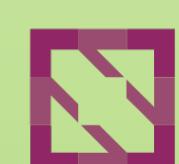
Savitha Raghunathan

Ian Coldwater

Tabitha Sable



KubeCon

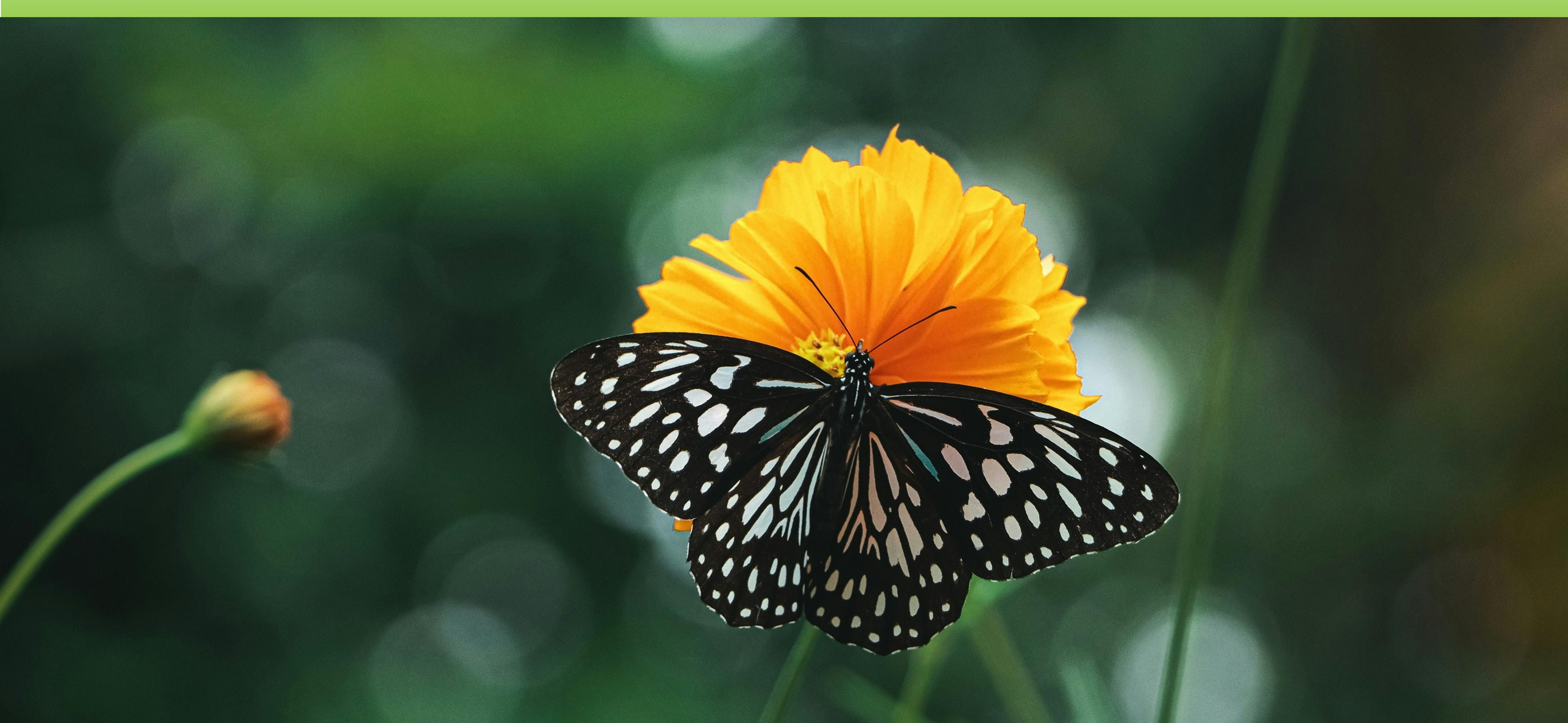


CloudNativeCon

North America 2025



KUBERNETES SIG SECURITY



EVOLUTION



SPREADING OUR WINGS



THIRD-PARTY AUDIT



SIG SECURITY DOCS



OWASP KUBERNETES TOP TEN



SIG Security is revamping the OWASP Kubernetes Top Ten!

We are planning to publish it by end of this year.

If you are interested in helping us curate the list and/or contribute to a section, please reach out to us via slack channel.

We want to hear from you!
Take the survey [here](#):



HARDENING GUIDE

Hardening guide - <https://github.com/kubernetes/sig-security/issues/30>

<https://kubernetes.io/docs/concepts/security/hardening-guide/scheduler/>

Documentation **Kubernetes Blog** **Training** **Careers** **Partners** **Community** **Ver**

[Kubernetes Documentation](#) / [Concepts](#) / [Security](#) / Hardening Guide - Scheduler Configuration

Hardening Guide - Scheduler Configuration

Information about how to make the Kubernetes scheduler more secure.

The Kubernetes [scheduler](#) is one of the critical components of the [control plane](#).

This document covers how to improve the security posture of the Scheduler.

A misconfigured scheduler can have security implications. Such a scheduler can target specific nodes and evict the workloads or applications that are sharing the node and its resources. This can aid an attacker with a [Yo-Yo attack](#): an attack on a vulnerable autoscaler.

kube-scheduler configuration

Scheduler authentication & authorization command line options

When setting up authentication configuration, it should be made sure that kube-scheduler's authentication remains consistent with kube-api-server's authentication. If any request has missing authentication headers, the [authentication should happen through the kube-api-server allowing all authentication to be consistent in the cluster](#).

- `authentication-kubeconfig` : Make sure to provide a proper kubeconfig so that the scheduler can retrieve authentication configuration options from the API Server. This kubeconfig file should be protected with strict file permissions.
- `authentication-tolerate-lookup-failure` : Set this to `false` to make sure the scheduler *always* looks up its authentication configuration from the API server.
- `authentication-skip-lookup` : Set this to `false` to make sure the scheduler *always* looks up its authentication configuration from the API server.
- `authorization-always-allow-paths` : These paths should respond with data that is appropriate for anonymous authorization. Defaults to

<https://kubernetes.io/docs/concepts/security/hardening-guide/authentication-mechanisms/>

Documentation **Kubernetes Blog** **Training** **Careers** **Partners** **Community** **Ver**

[Kubernetes Documentation](#) / [Concepts](#) / [Security](#) / Hardening Guide - Authentication Mechanisms

Hardening Guide - Authentication Mechanisms

Pod Security Policies
Security For Linux Nodes
Security For Windows Nodes
Controlling Access to the Kubernetes API
Role Based Access Control Good Practices
Good practices for Kubernetes Secrets
Multi-tenancy
Hardening Guide - Authentication Mechanisms
Hardening Guide - Scheduler Configuration
Kubernetes API Server Bypass Risks
Linux kernel security constraints for Pods and containers
Security Checklist
Application Security Checklist

- `Policies`
- `Scheduling, Preemption and Eviction`
- `Cluster Administration`
- `Windows in Kubernetes`
- `Extending Kubernetes`

X.509 client certificate authentication

Kubernetes leverages [X.509 client certificate](#) authentication for system components, such as when the kubelet authenticates to the API Server. While this mechanism can also be used for user authentication, it might not be suitable for production use due to several restrictions:

HARDENING GUIDE

Examples:

- Threat Model
- API Server Configuration
- Controller Manager Configuration
- File Permissions
- Worker Node Configuration
- PKI Management
- Authorization
- Workload Security Configuration
- Network Policy Configuration
- Add-On Configuration
- etcd

BRING YOUR IDEAS



If you have an idea to improve the security content of the Kubernetes website, please feel free to start a thread in the [Slack channel](#) and/or create an issue in the [k/website](#) repo.

TOOLING



TOOLING



SELF-ASSESSMENTS



SELF-ASSESSMENTS 101

Define the scope

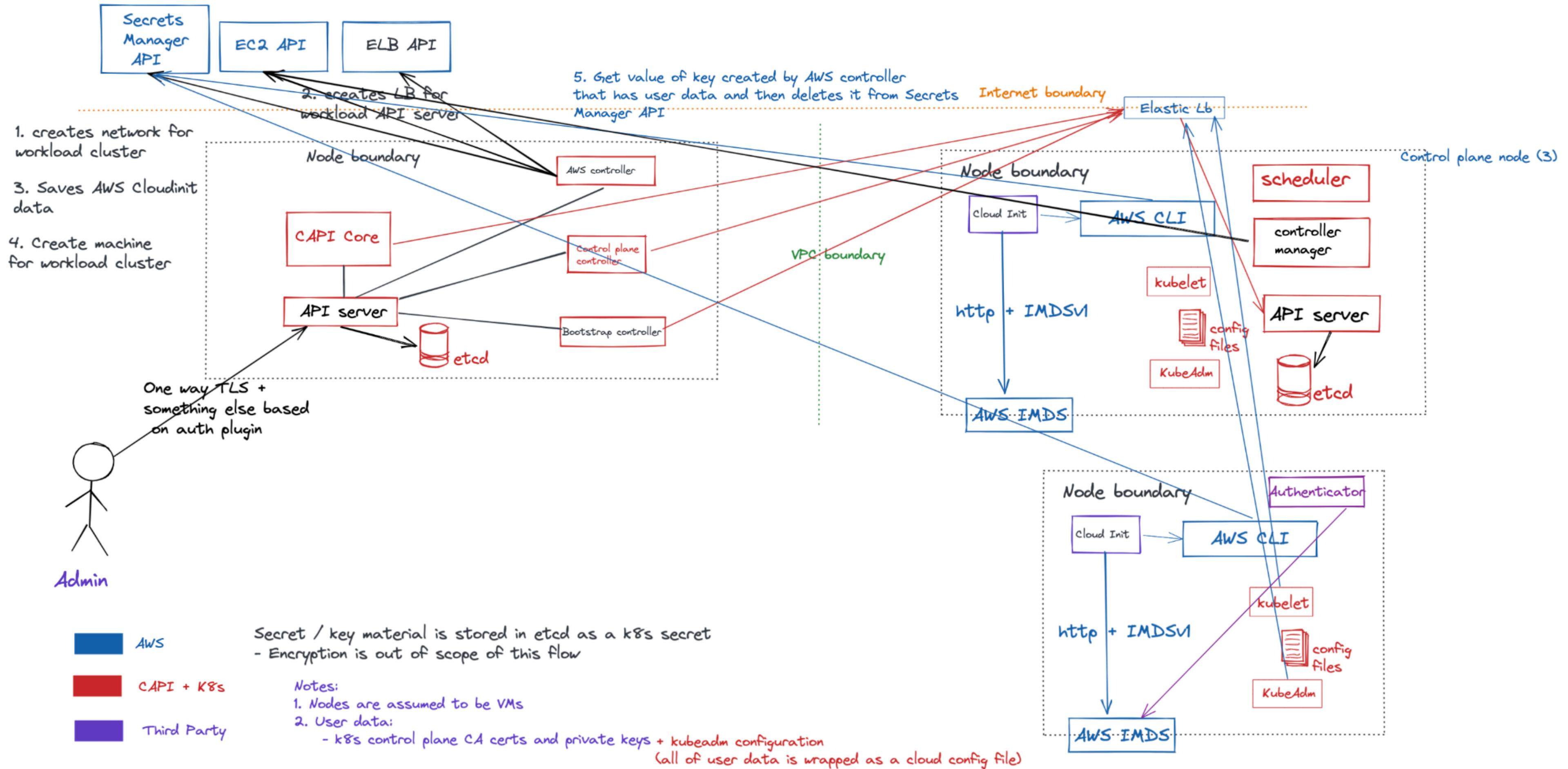
- What workflows are used most?
- What workflows does the community want a security assessment of?

Data Stores and Data flow Diagram (DFD)

Threat Modeling with STRIDE

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service (DoS)
- Elevation of Privilege

DATA FLOW DIAGRAM



ETCD ASSESSMENT



JOIN TO COLLABORATE!



BUTTERFLY EFFECT

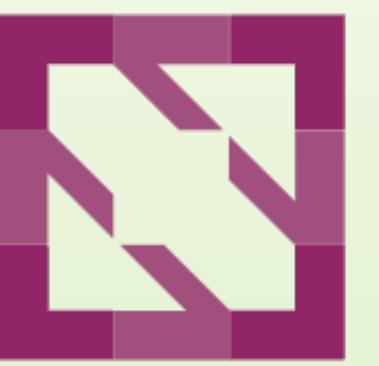


GET INVOLVED!





KubeCon



CloudNativeCon

North America 2025

