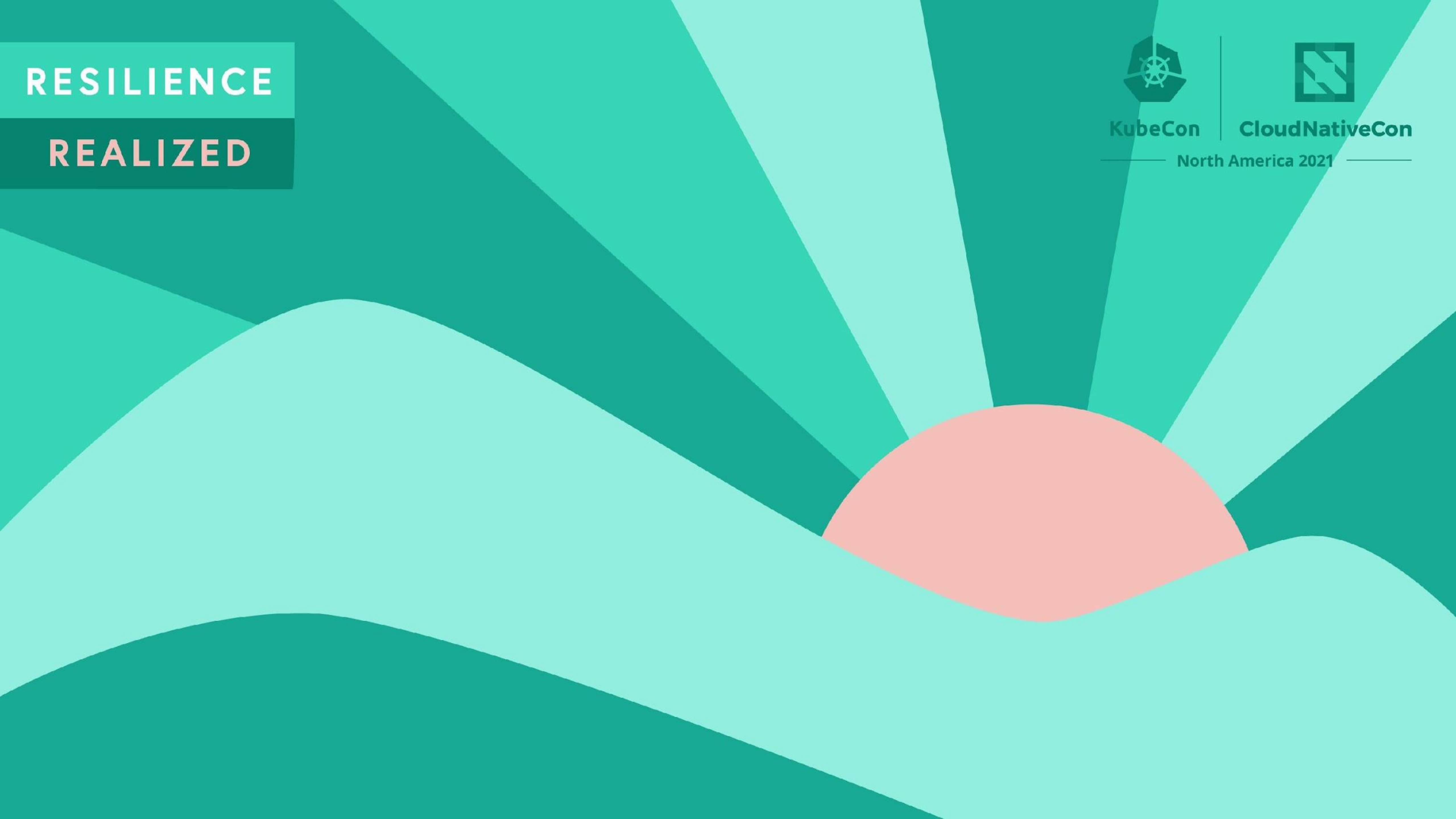


RESILIENCE

REALIZED

KubeCon | CloudNativeCon

North America 2021

Security Through Transparency:

Kubernetes SIG Security Update

Ian Coldwater, Twilio
Pushkar Joglekar, VMware
Rey Lejano, SUSE
Savitha Raghunathan, Red Hat

Security Through Transparency:

Kubernetes SIG Security Update

KubeCon | CloudNativeCon

North America 2021

October 11-15, 2021

Ian Coldwater
Security Architect
Twilio

Pushkar Joglekar
Sr Security Engineer
VMware

Rey Lejano
Field Engineer
SUSE

Savitha Raghunathan
Sr Software Engineer
Red Hat

Introduction

What we’ll cover:

- What is SIG Security
- Subproject current activities
- What’s next for subprojects
- How to get involved

Who We Are?

- What is SIG Security?
    - Horizontal SIG that covers security initiatives for the entire Kubernetes project
        - core components
        - tooling e.g. scanning
        - security documentation
        - vulnerability management
        - security community management

Our Subprojects

- security-docs
    - Security Documents and Documentation
- security-audit
    - Third-party Security Audit
- security-tooling
    - Development and Enhancements of Security Tooling
- security-self-assessment
    - Introspection to Increase Security Position

Documentation

- Sub Project Goals:

  - Collaborate and create/improve existing security content for Kubernetes documentation.
  - Keep the documentation and security examples up to date.
  - Create security awareness through documentation.

- Current Projects:

  - Blog related to NSA/CISA Kubernetes hardening guide.
  - Admission control threat model.
  - Ongoing updates to the Kubernetes website.

Docs: What’s Next?

- Future Projects:

  - Kubernetes security checklist for cluster creation and deployment.
  - Kubernetes RBAC guide and tutorial.

- sig-security-docs project is looking for volunteers!

- If you have any an idea to improve the security content, please feel free to start a thread in the slack channel.

Third-Party Security Audit

Subproject Goals:

- Coordinate regular, comprehensive, third-party security audits

Audit Goals:

- Identify vulnerabilities or weaknesses in Kubernetes
- Make Kubernetes more secure

Audit Roadmap:

- Kubernetes is a large project (146 enhancements in the last 3 minor releases)
- An audit roadmap is designed to guide the focus areas of future audits

Third-Party Security Audit

Audit Scope:

- kube-apiserver
- kube-scheduler
- etcd, Kubernetes use of
- kube-controller-manager
- cloud-controller-manager
- kubelet
- kube-proxy
- secrets-store-csi-driver

Third-Party Security Audit: What's Next?

- What's Next with Third-Party Security Audits:
  - Increase breadth of third-party party security audits, outside the scope scope of core Kubernetes components

- Self-assessments and Audit Roadmap (more about self-assessments in a few minutes):
  - Not required to be part of a third-party security audit but self-assessment of a component or focus area strengthens it's security posture for a more effective third-party security audit

Tooling

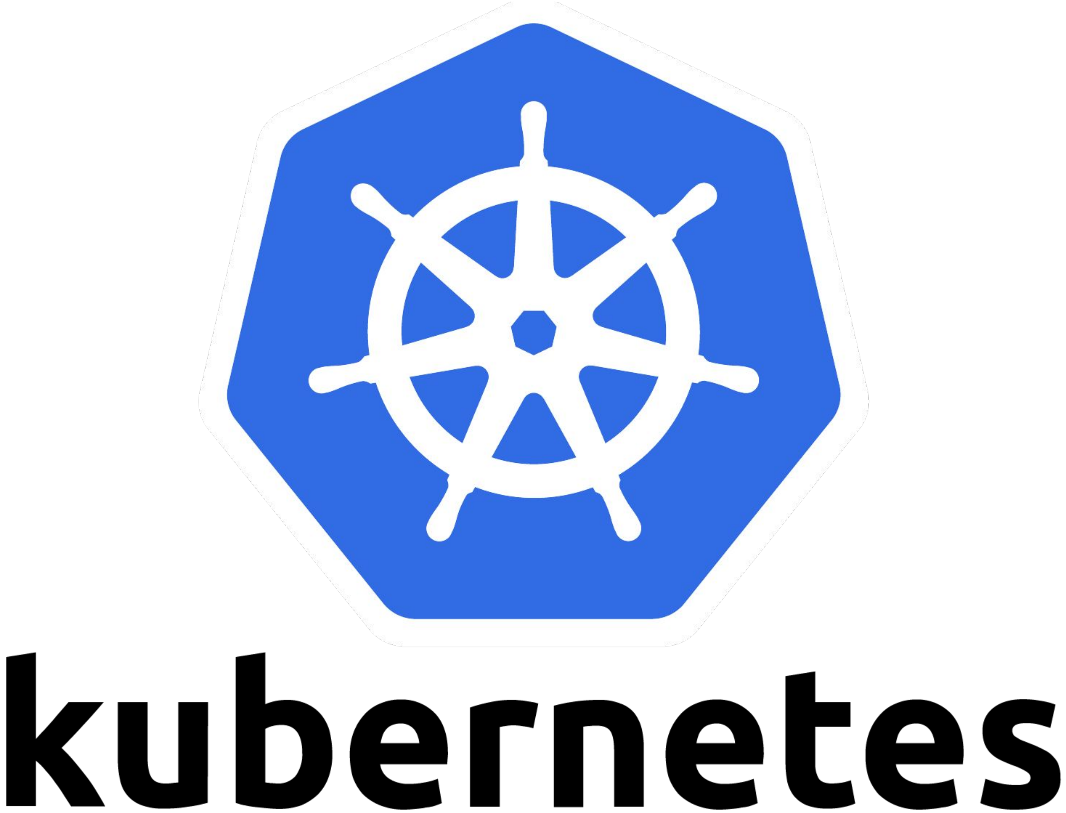
- Leading:
  - Vulnerability Management of known vulnerabilities
    - Build Time Dependency Scanning
    - Container Image scanning
  - Auto-refreshing fixed CVE feed
- Helping:
  - PSP replacement
  - Bumping Container Base Images & Dependencies
  - Learning Sessions

Tooling: What’s Next?

- Leading:
  - Triage Policy and Process
  - Shadow Program for Triage
  - Reducing gap between MTTD and MTTR
- Helping:
  - SBoM for K8s
  - KEP Reviews
- And anything that *you* would like us to do!!
  - Hit us up on #sig-security-tooling

Security Self-Assessments

Cross Collaboration with CNCF Security TAG



Security Self-Assessments

- Scoped to Kubernetes Sub-Projects
- First assessment: Cluster API (Jan 2022)
    - Help welcome !!
- Intake-form via Github Issues
- Community Driven: Everyone new or experts are welcome!

How You Can Get Involved?

- SIG Meeting: bi-weekly on Thursdays at 9am Pacific
- Slack channel: #sig-security
- Find more about SIG Security on GitHub: https://github.com/kubernetes/community/tree/master/sig-security

Q & A