

CLOUDNATIVE
SECURITYCON
NORTH AMERICA 2024
JUNE 26-27 | SEATTLE, WA #CNSCon

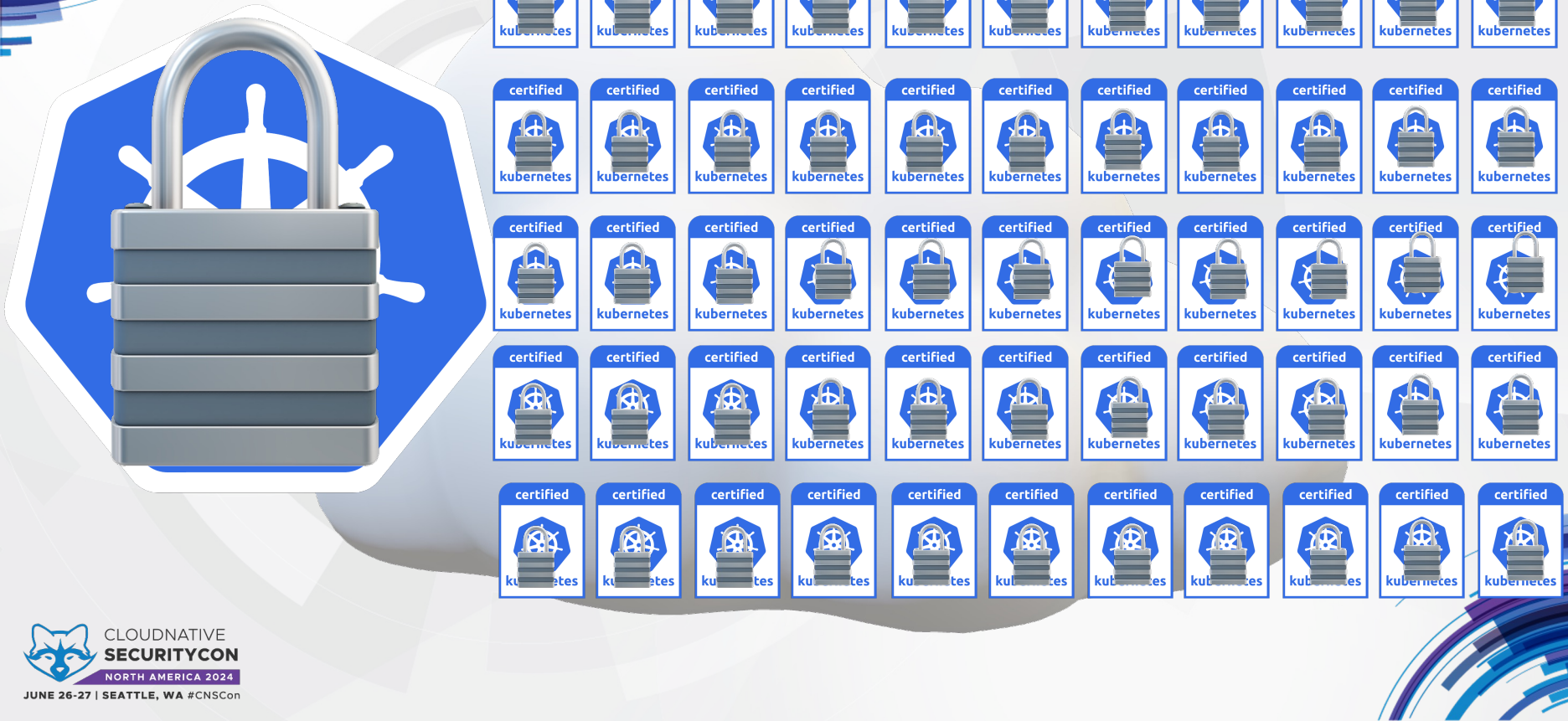
Keynote: Securing Kubernetes, the Upstream Way

Rey Lejano, Red Hat

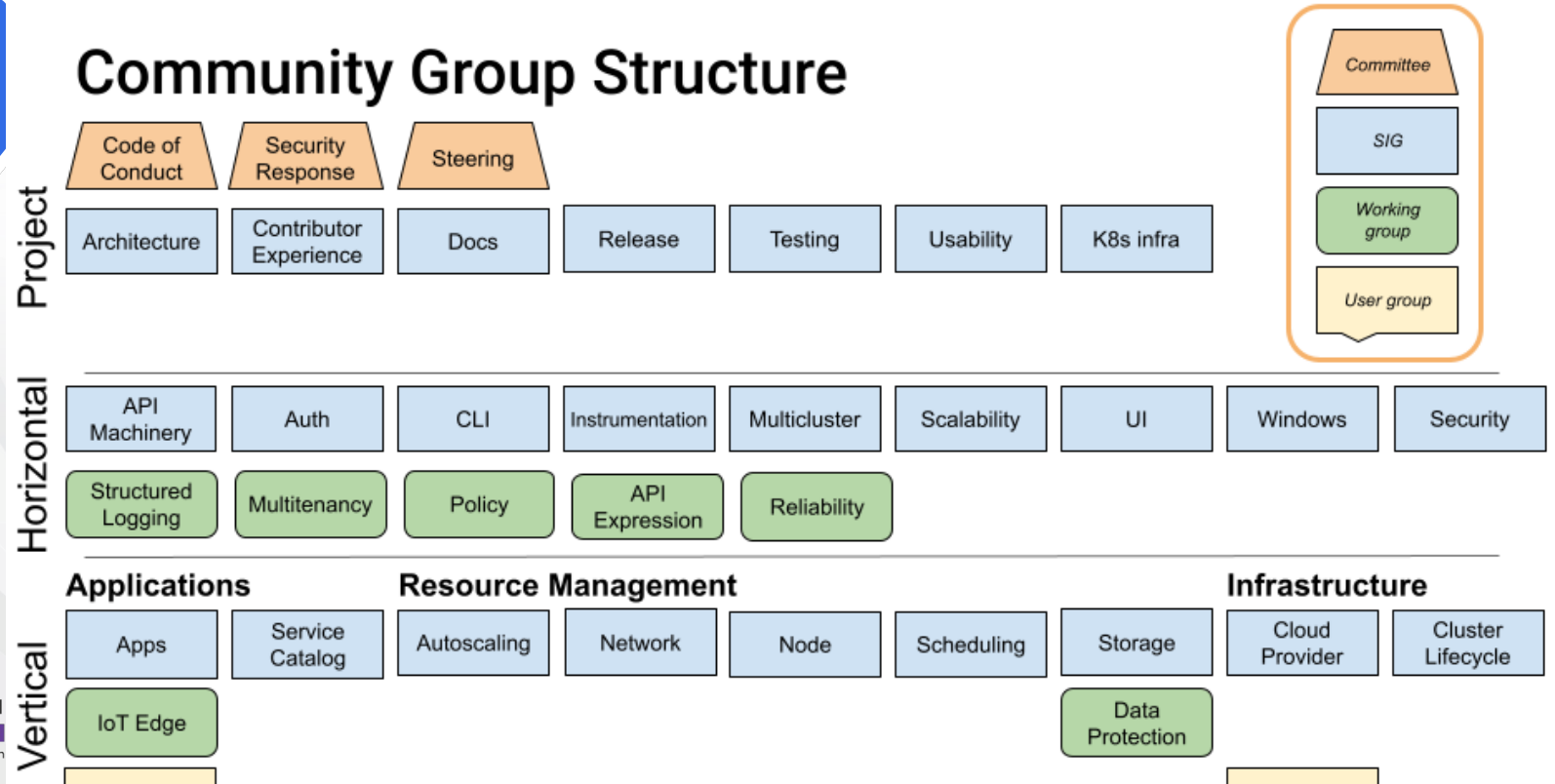
Cloud Native Security



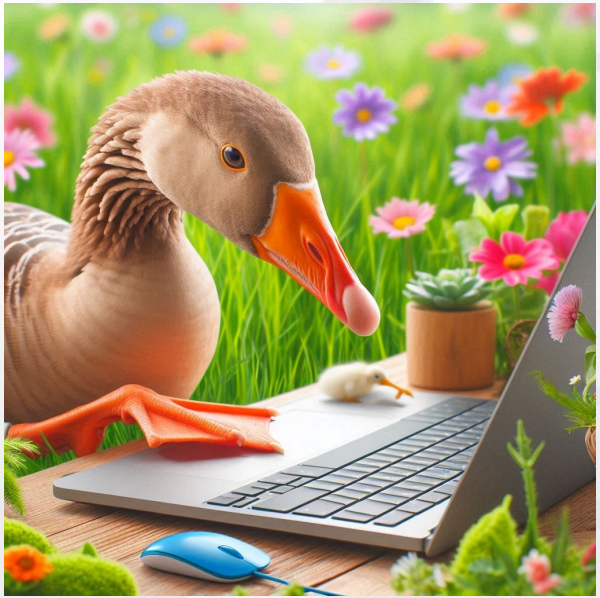
Cloud Native Security



Kubernetes SIG Security

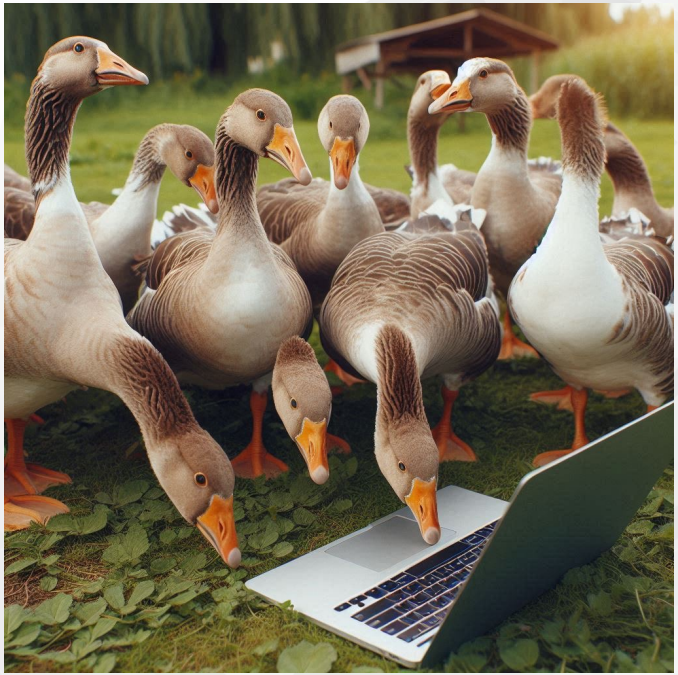


Kubernetes SIG Security History



- Grew out of the Third-Party Security Audit Working Group
- Goal is to improve the security of the Kubernetes project

Kubernetes SIG Security Today

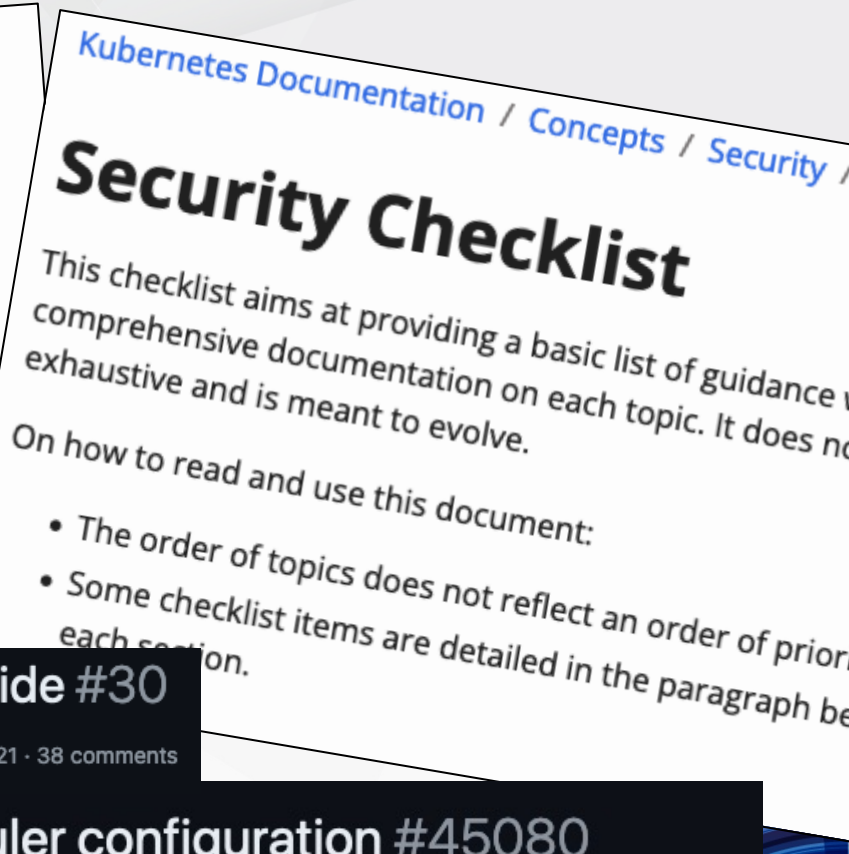


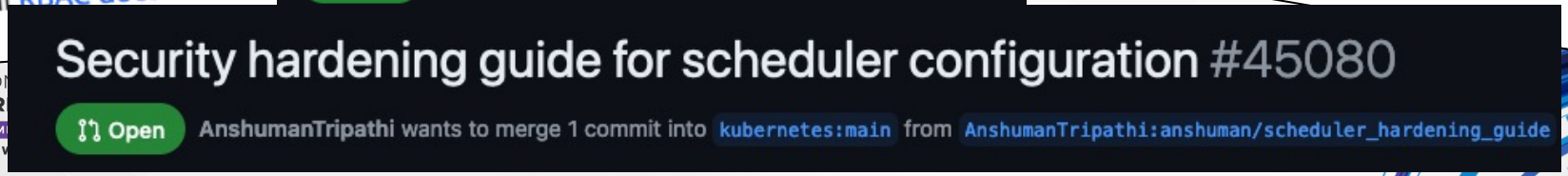
4 subprojects:

- Security Docs
- Security Tooling
- Self-Assessments
- Third-Party Security Audit

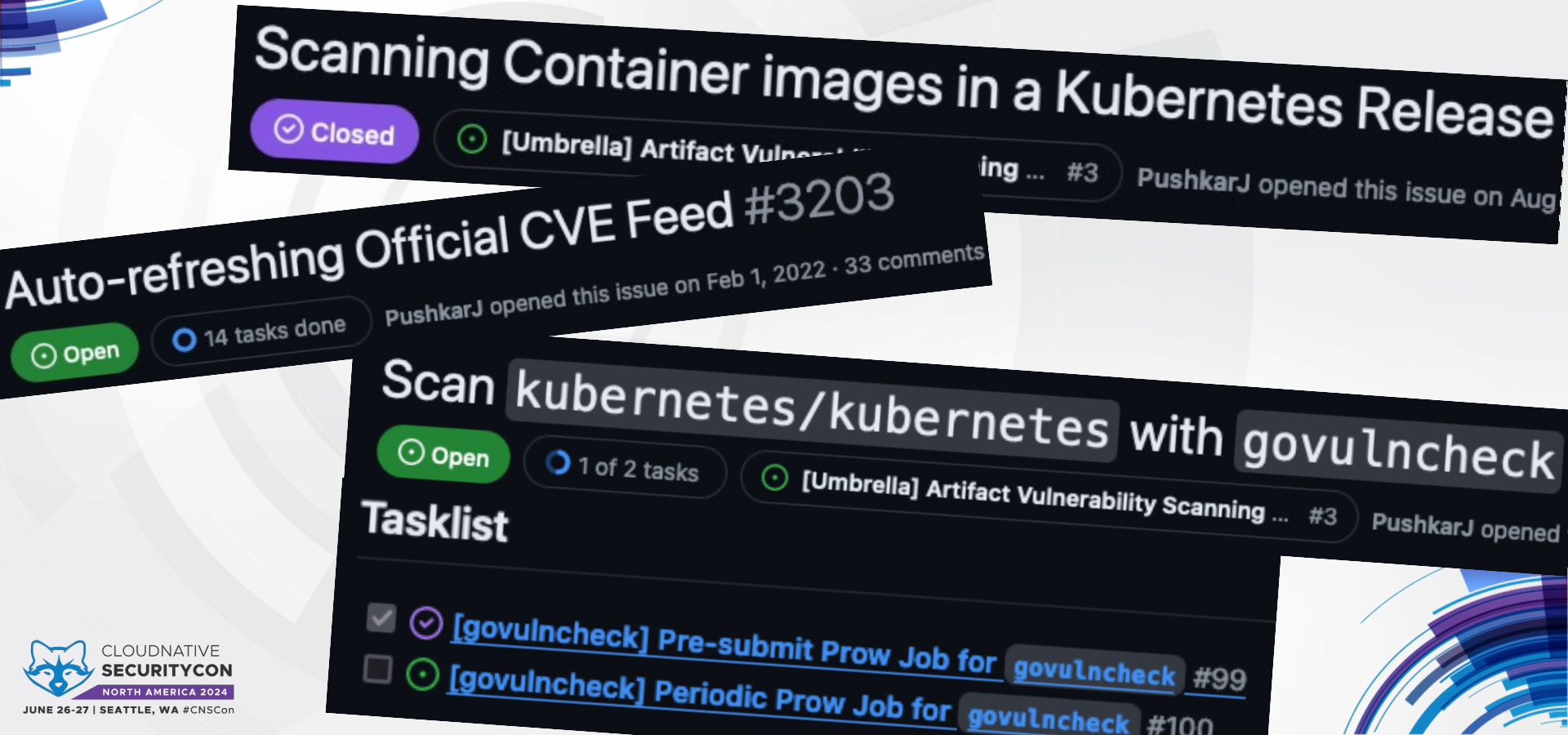
Security Docs







Security Tooling



Self-Assessments

Cluster API Security Self-Assessment

Metadata

- **Last Modified:** 2022-03-02
- **Youtube Recordings:** Cluster API Secu
- **Authors** (alphabetical order):
  - Ankita Swamy
  - Naadir Jeewa
  - Pushkar Joglekar
  - Robert Ficcaglia
- **Reviewers** (alphabetical order):
  - Fabrizio Pandini
  - Lubomir I. Ivanov
  - Stefan Büringer



Third-Party Security Audit





2019 Third-Party Security Audit



Key findings:

Issue 6: Bearer tokens revealed by logs

- Fixed: hid bearer tokens in logs

Issue 9: Environment variables expose sensitive data

- Fixed: moved password retrieval to test

Issue 22: iSCSI volume storage cleartext secrets in logs

- Fixed: removed iSCSI volume storage cleartext secrets in logs

Motivated a

long term preventative solution

Enhancement #1933: Defend against logging static analysis

- Added go-flow-levee to Prow's testing of PRs to stop secret logging
- Graduated in v1.23

v1.24 (2023) Third-Party Security Audit

Key findings:

Issue 5: Common Certificate Authority Possible for Client CA and Request Header CA

- Under a specific condition, an authenticated user can have privileges escalated to cluster admin

Issue 6: Path Traversal in Namespace Specifier

- Users can bypass access controls by passing directory traversal sequence (..) as the namespace in a request to the Kubernetes API.
- Fixed: added a check on namespace identifier in API requests

v1.24 (2023) Third-Party Security Audit

Key findings:

Issue 7: Redirection of API Server Traffic to kubelet (privilege escalation)

- A user can get cluster-admin permissions by proxying request through the API server to workloads or nodes and if the API server recognizes the proxy target as a kubelet

Issue 18: Privilege Escalation via node/proxy Permission

- A user with get and create permissions for nodes/proxy in a cluster can proxy requests through the API server will have full permissions on the kubelet API and can execute any commands in any Pod

What we learned

- Kubernetes is not perfect
- Kubernetes is not secure by default
- Takes a community to secure upstream Kubernetes

