A Raccoon and a group of Turtles Secure Clusters together!

KubeCon | CloudNativeCon
North America 2022

BUILDING FOR THE ROAD AHEAD

DETROIT 2022

October 24-28, 2022

Pushkar Joglekar
Tech Lead
CNCF TAG Security

Naadir Jeewa
Staff Engineer for Tanzu Kubernetes Grid
VMware

What's with the animals?

Raccoon
=
CNCF TAG Security

Image credits: cncf/artwork and unsplash

What's with the animals?

Geese

=

Kubernetes
SIG Security

What's with the animals?

Turtles
=
Kubernetes
Cluster API

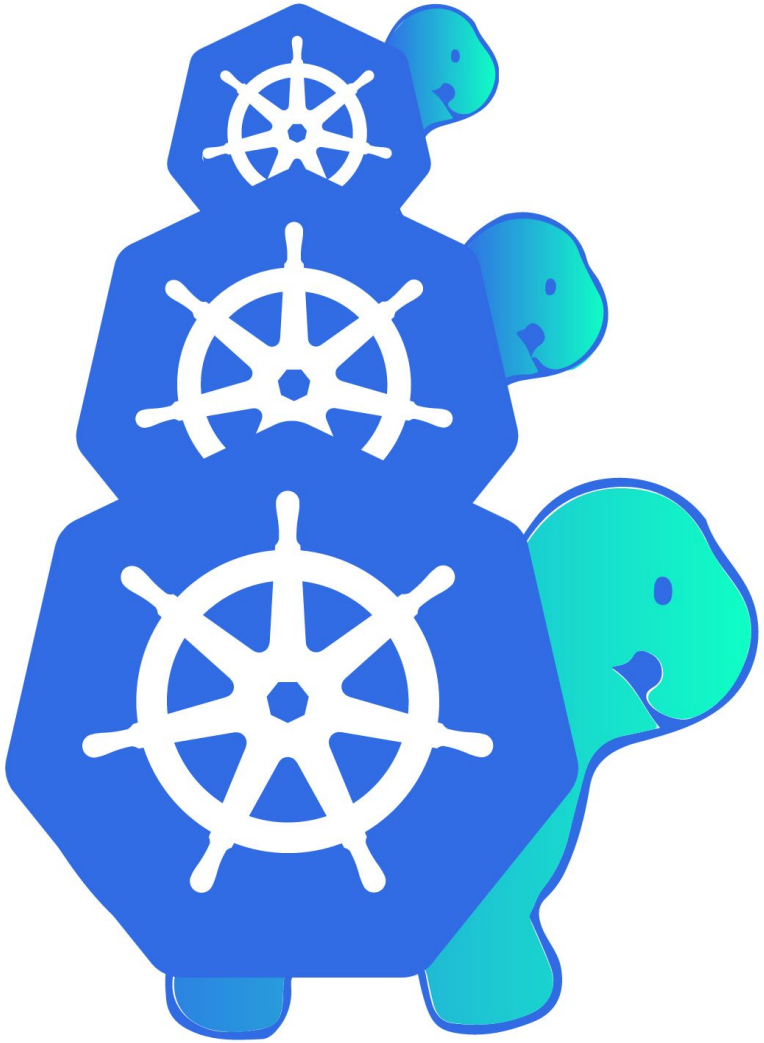
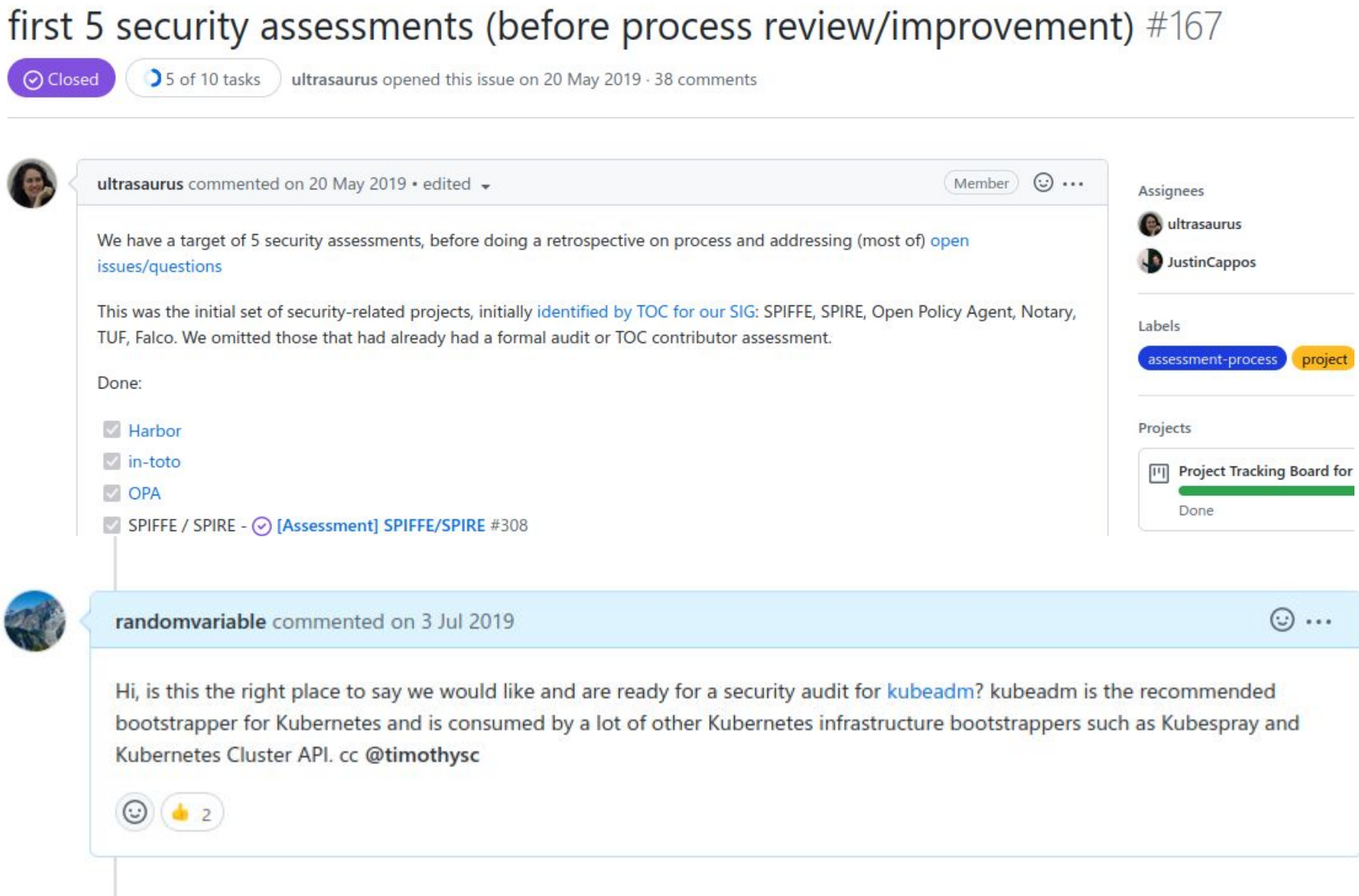


Image credits: kubernetes-sigs/cluster-api

How it started?

The heady days of 2019…



first 5 security assessments (before process review/improvement) #167

Closed · 5 of 10 tasks · **ultrasaurus** opened this issue on 20 May 2019 · 38 comments

ultrasaurus commented on 20 May 2019 • edited · Member

We have a target of 5 security assessments, before doing a retrospective on process and addressing (most of) open issues/questions

This was the initial set of security-related projects, initially identified by TOC for our SIG: SPIFFE, SPIRE, Open Policy Agent, Notary, TUF, Falco. We omitted those that had already had a formal audit or TOC contributor assessment.

Done:

- [x] Harbor
- [x] in-toto
- [x] OPA
- [x] SPIFFE / SPIRE - [Assessment] SPIFFE/SPIRE #308

Assignees: ultrasaurus, JustinCappos

Labels: assessment-process, project

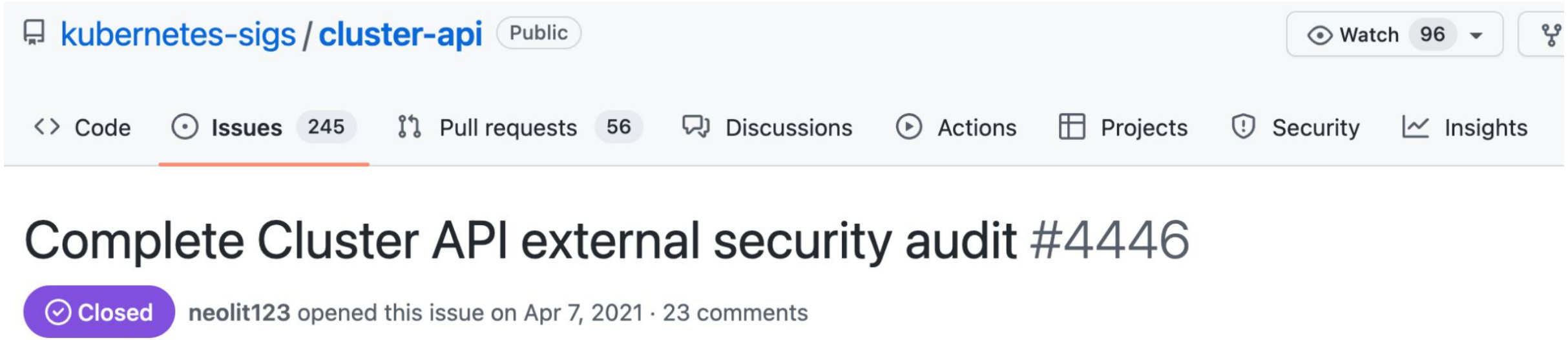
Projects: Project Tracking Board for … Done

randomvariable commented on 3 Jul 2019

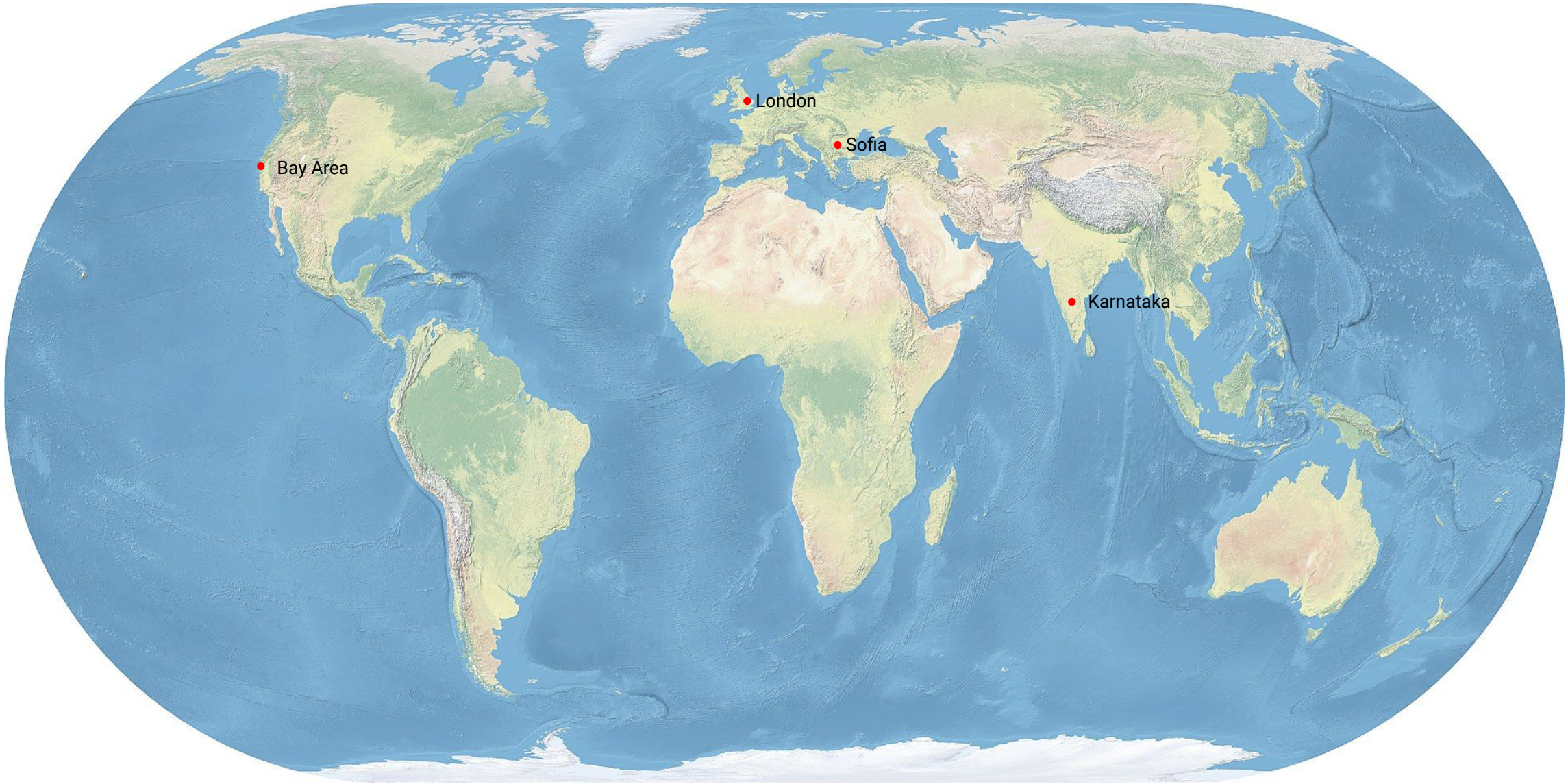
Hi, is this the right place to say we would like and are ready for a security audit for kubeadm? kubeadm is the recommended bootstrapper for Kubernetes and is consumed by a lot of other Kubernetes infrastructure bootstrappers such as Kubespray and Kubernetes Cluster API. cc **@timothysc**

2

How it started?

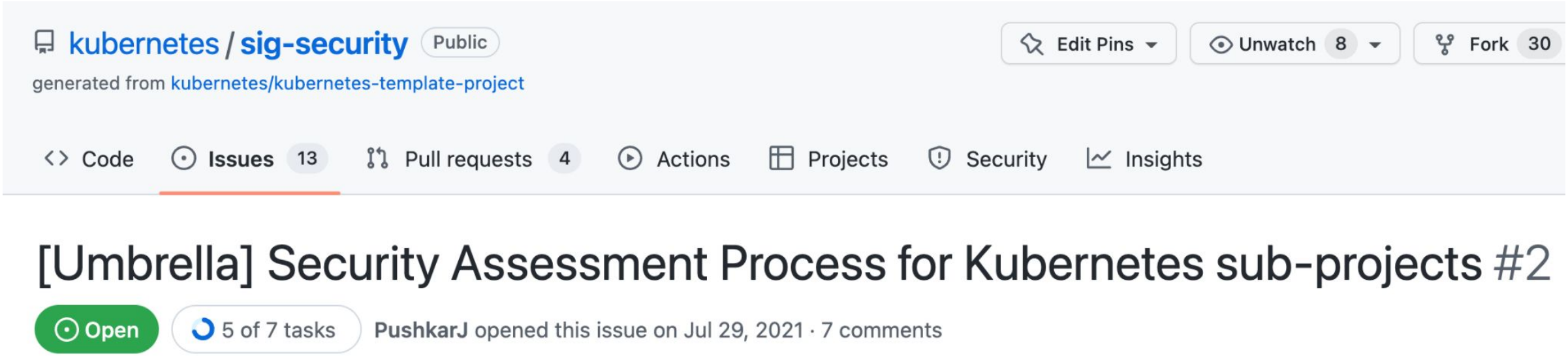


Time zones



How it started?

How it started?



To Sync or Async?

May 22nd, 2021

Slack channel created

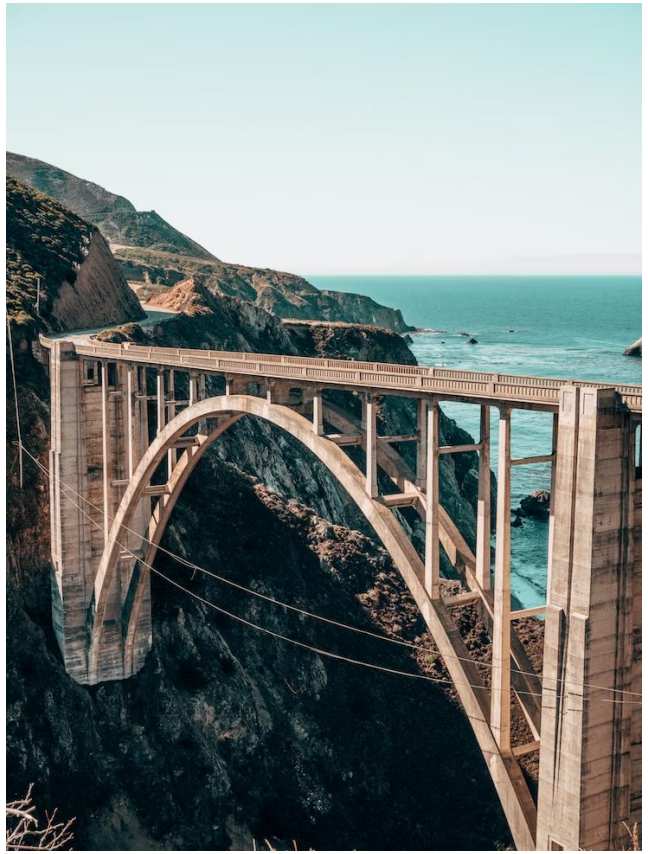


Image Credits: https://unsplash.com/photos/Hp5Acad1H0k

August 26th, 2021

First Meeting Planned

Async First

New channel for security assessment of cluster api #5792

Merged **k8s-ci-robot** merged 2 commits into `kubernetes:master` from `PushkarJ:patch-1` on May 22, 2021

sig-security-assess-capi

★ Get Notifications for All Messages Start a Call

About Members 80 Integrations Settings

Topic Edit

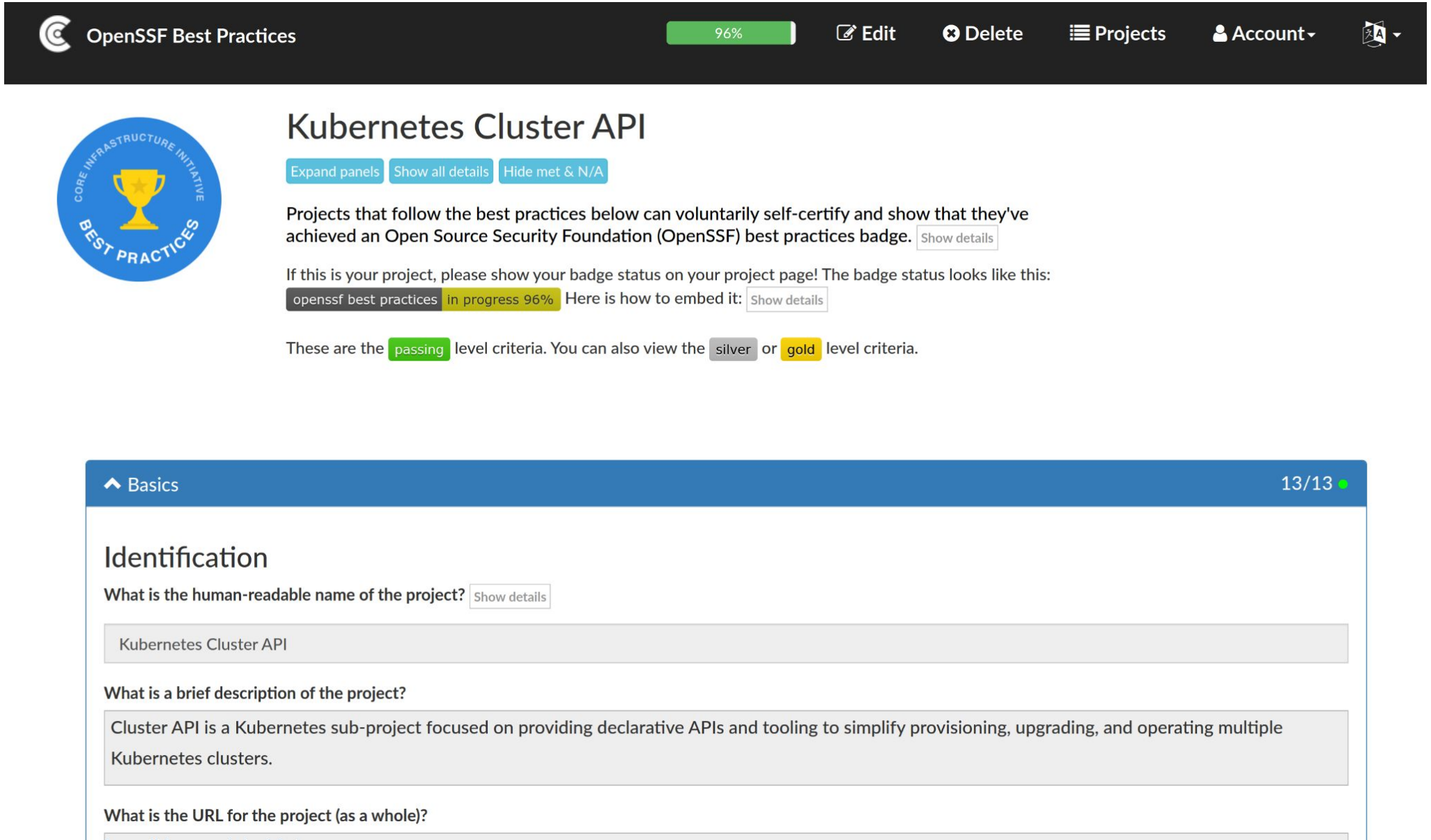
Working doc: https://bit.ly/3wJMWCr

Minutes: https://bit.ly/3eXr5AL

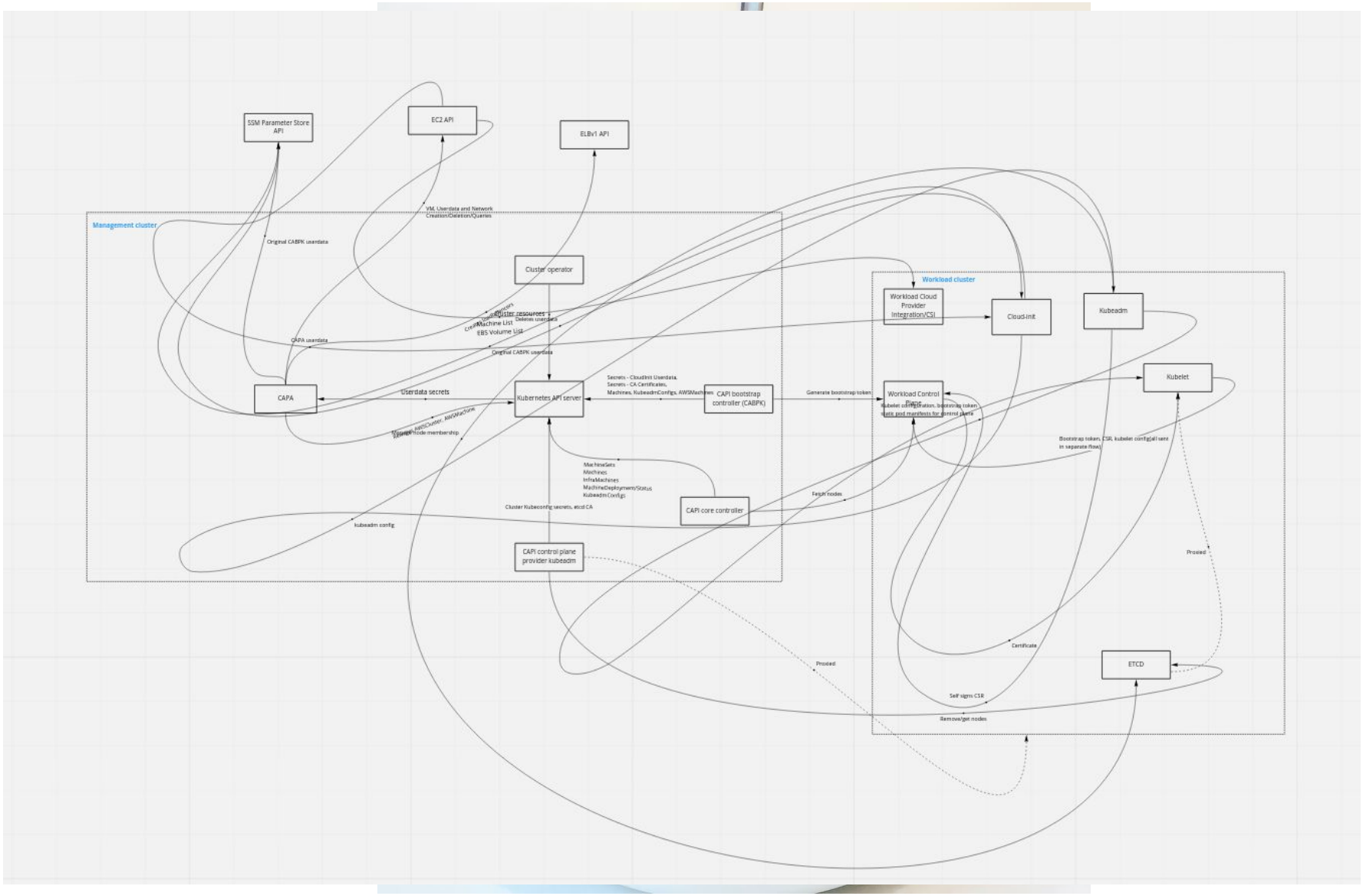
Description Edit

Affiliated with #sig-security

Low hanging fruit for OSS projects



Data Flow Diagrams



Scoping

Some of the possibilities

- The operating system
- All of the cloud providers: AWS/Azure/Google/vSphere/OpenStack etc…
- Hardware trust systems
- Tenancy boundaries
- Core Kubernetes components
  - kubelet
  - kube-controller-manager
- Certificates!!

What's already done

- Kubernetes security review
  - Covers core componentry
- Cloud providers
  - AWS shared responsibility model

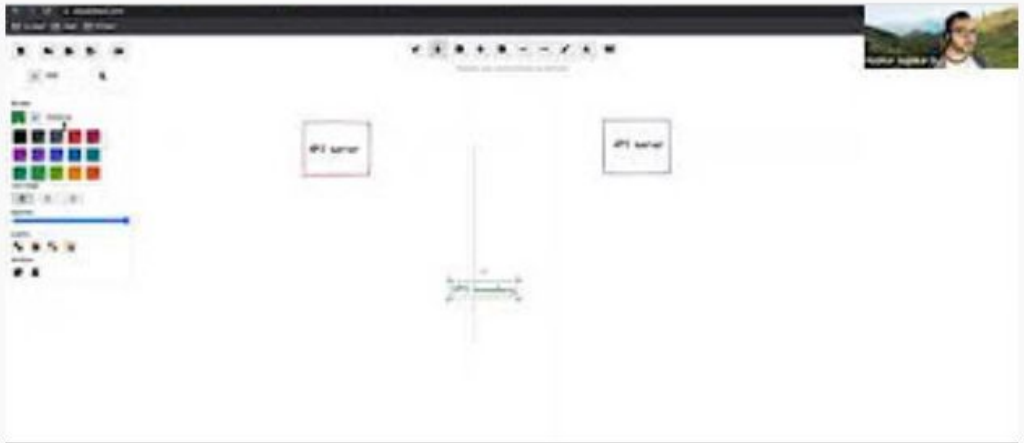
Where do the project contributors skills and primary contributions lie

- kubeadm
- AWS Networking & Security

Reasonable scope

- Take a slice through system:
  - Machine bootstrapping
  - Control plane bootstrapping

In Sync too



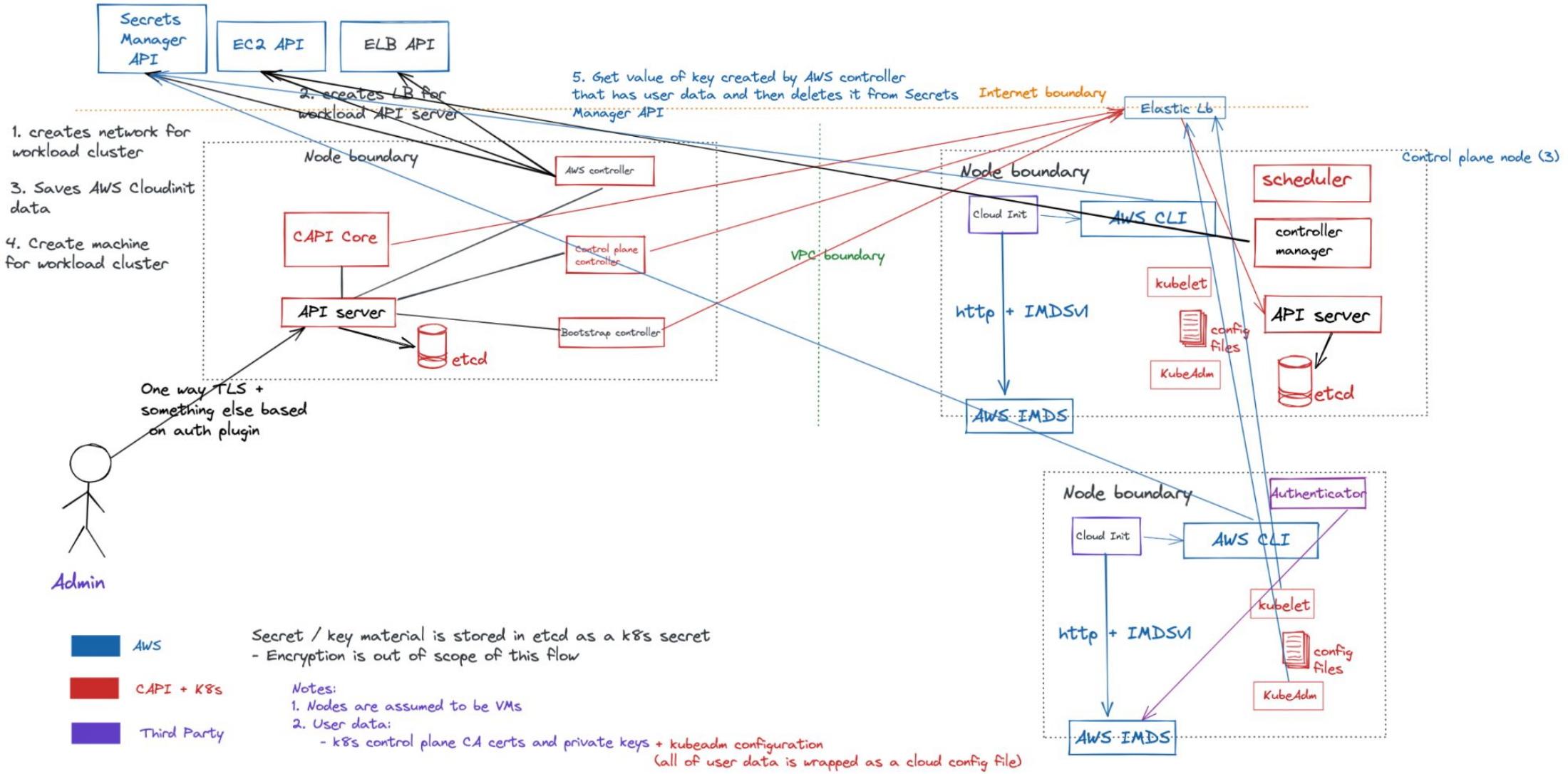
PLAY ALL

Kubernetes SIG Security Self-Assessments

5 videos • 32 views • Last updated on Feb 23, 2022

Public

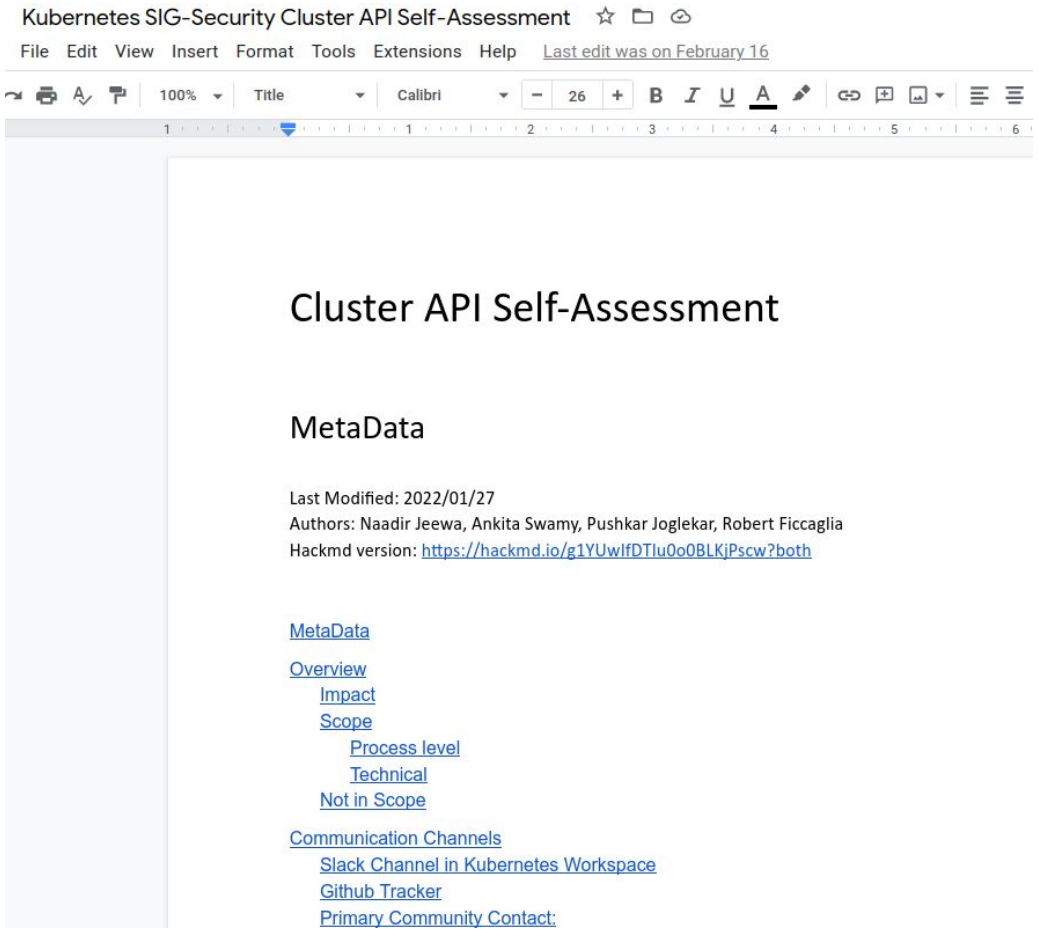
Data Flow Diagrams



Pre-drafts

A Google doc created, based on a template

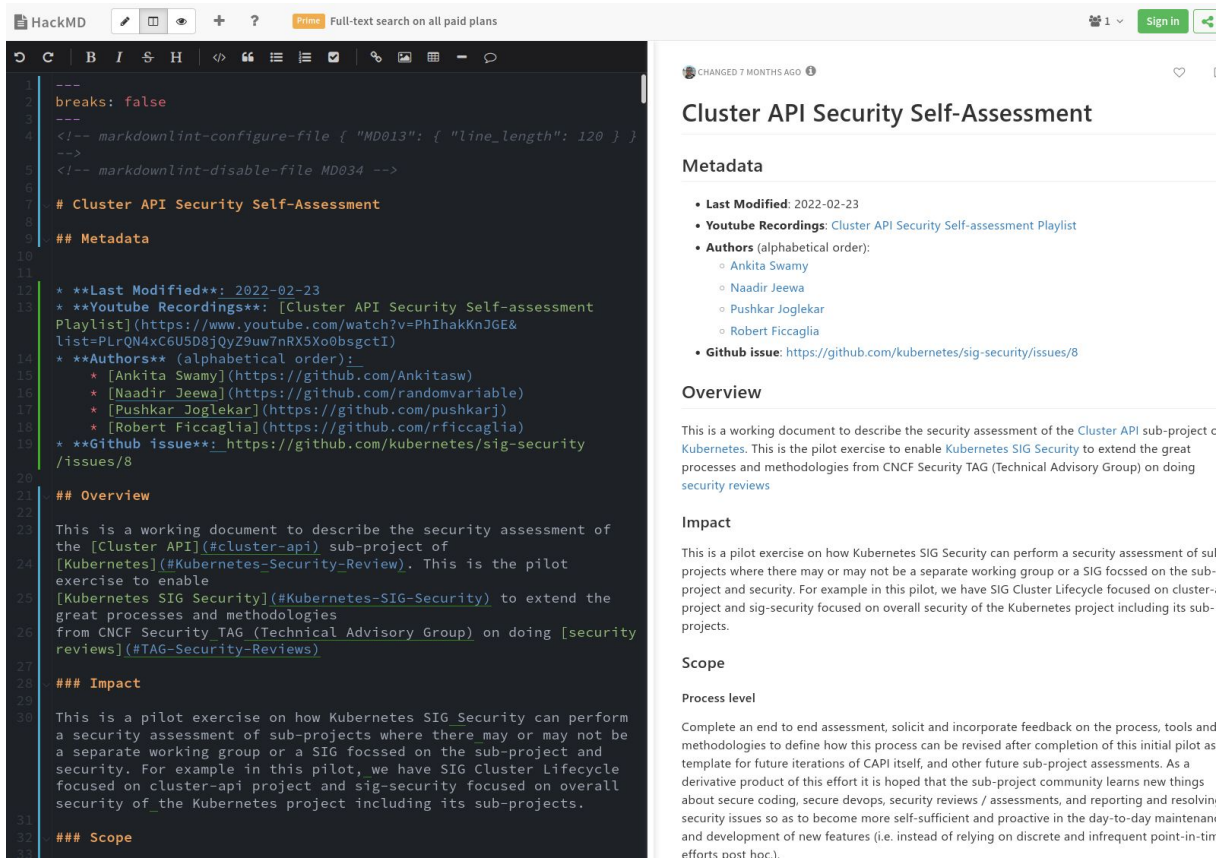
https://bit.ly/capi-sa-draft



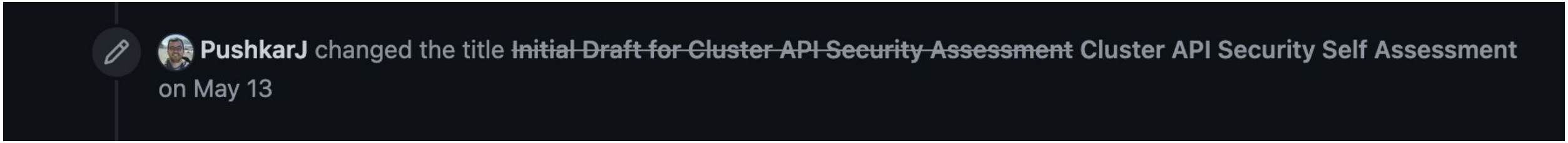
Pre-drafts

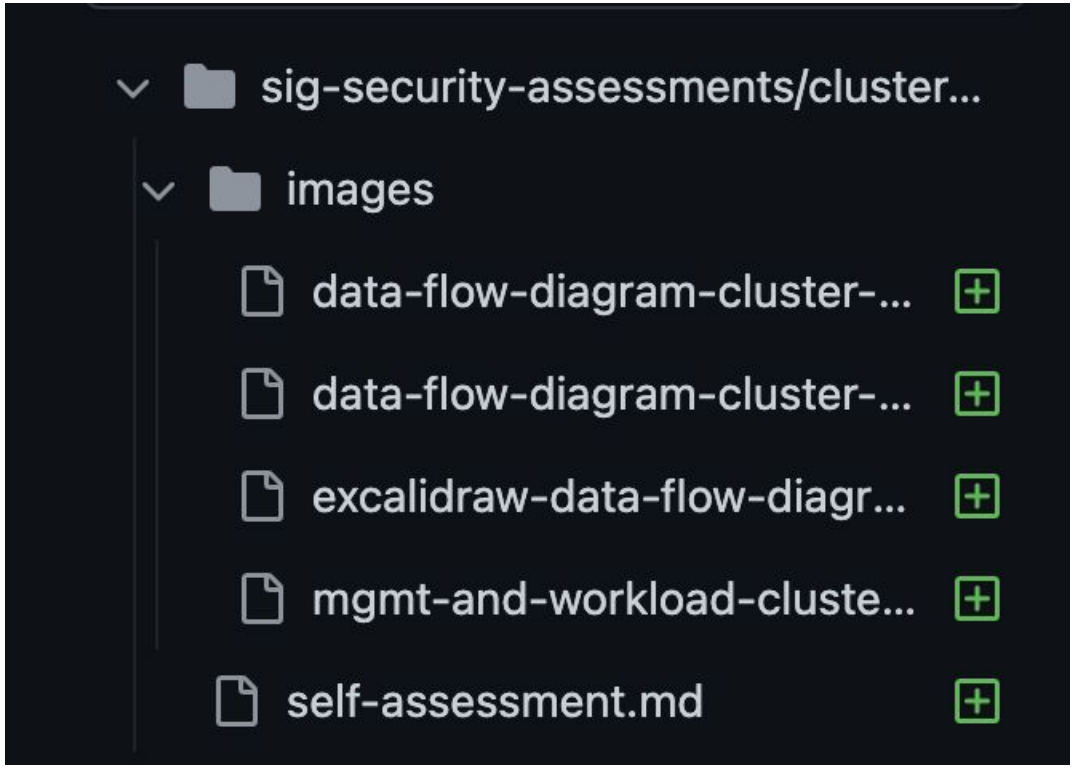
In preparation for the final pull request, we moved to HackMD

https://bit.ly/capi-sa-hackmd

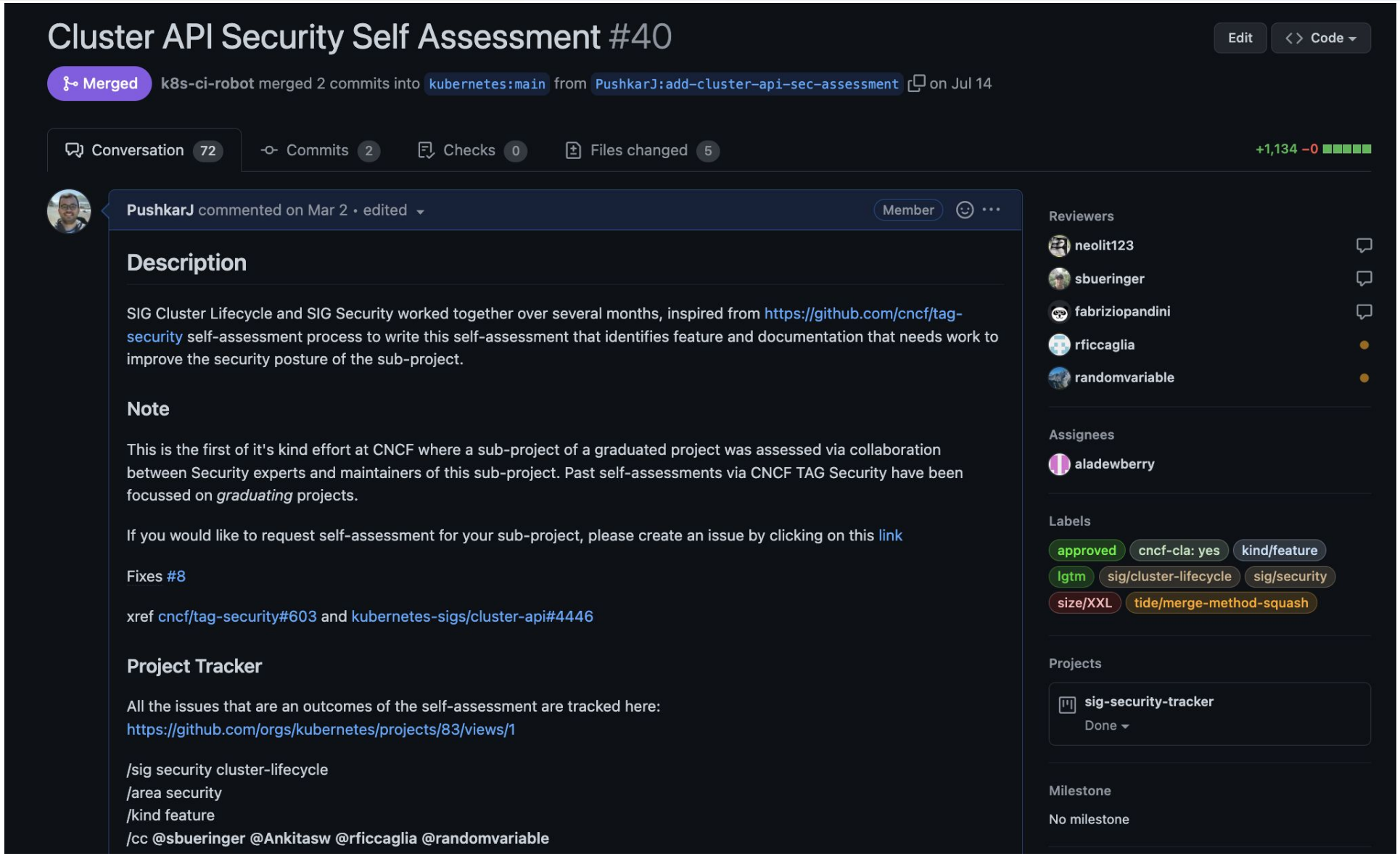


Draft PRs


PushkarJ changed the title ~~Initial Draft for Cluster API Security Assessment~~ Cluster API Security Self Assessment
on May 13


sig-security-assessments/cluster...
images
data-flow-diagram-cluster-...
data-flow-diagram-cluster-...
excalidraw-data-flow-diagr...
mgmt-and-workload-cluste...
self-assessment.md

PR Reviews



Cluster API Security Self Assessment #40

Edit | Code

Merged | k8s-ci-robot merged 2 commits into `kubernetes:main` from `PushkarJ:add-cluster-api-sec-assessment` on Jul 14

Conversation 72 | Commits 2 | Checks 0 | Files changed 5 | +1,134 −0

PushkarJ commented on Mar 2 • edited — Member

Description

SIG Cluster Lifecycle and SIG Security worked together over several months, inspired from https://github.com/cncf/tag-security self-assessment process to write this self-assessment that identifies feature and documentation that needs work to improve the security posture of the sub-project.

Note

This is the first of it's kind effort at CNCF where a sub-project of a graduated project was assessed via collaboration between Security experts and maintainers of this sub-project. Past self-assessments via CNCF TAG Security have been focussed on *graduating* projects.

If you would like to request self-assessment for your sub-project, please create an issue by clicking on this link

Fixes #8

xref cncf/tag-security#603 and kubernetes-sigs/cluster-api#4446

Project Tracker

All the issues that are an outcomes of the self-assessment are tracked here:
https://github.com/orgs/kubernetes/projects/83/views/1

/sig security cluster-lifecycle
/area security
/kind feature
/cc **@sbueringer @Ankitasw @rficcaglia @randomvariable**

Reviewers
- neolit123
- sbueringer
- fabriziopandini
- rficcaglia
- randomvariable

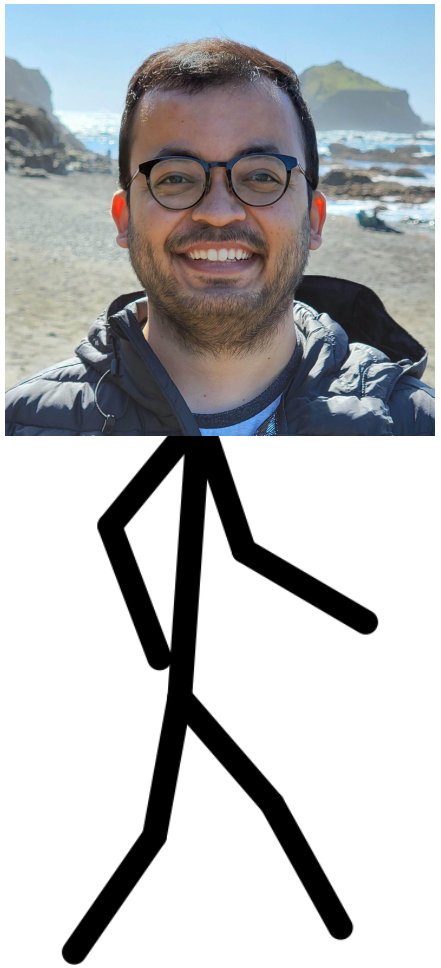
Assignees
- aladewberry

Labels
approved | cncf-cla: yes | kind/feature | lgtm | sig/cluster-lifecycle | sig/security | size/XXL | tide/merge-method-squash

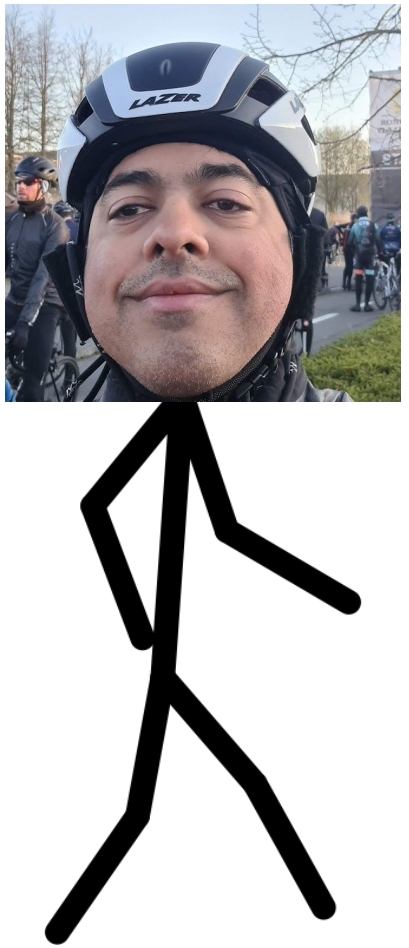
Projects
sig-security-tracker
Done

Milestone
No milestone

Changes: Roles and Responsibilities



- Moved from 50/50 downstream + upstream split to 30/70 split in favor of upstream - yay!
- New sub-project was formed to ensure this process can be repeatable for future sub-project self-assessments



- Moved from upstream to work on downstream
- Found replacements who would continue working as SMEs of cluster-api

https://sched.co/1BvfI

Fuzz Testing

KubeCon CloudNativeCon North America 2022

Security Self Assessment: [DEV-3] Setup Cluster API on oss-fuzz #6059

Closed **randomvariable** opened this issue on Feb 3 · 11 comments

randomvariable commented on Feb 3 — Member

This is a follow up from the CAPI security self assessment meeting of 2022/02/02, where we had an introduction to CNCF sponsored fuzz testing from **@DavidKorczynski** and **@raesene**

- Adding Cluster API to the CNCF Fuzzing setup is nominally approved
- Initial work would be about a month, and normally done directly in the above repository to prevent the need to wait for PR reviews. However, CAPI should strongly consider porting the fuzz tests over to CAPI repository after the initial work is done.
- Cluster API would be integrated into OSS-Fuzz for continuous fuzzing with results viewable in bugs.chromium.org
- The fuzz testing could potentially uncover a lot of bugs (see example for Envoy) and will need to be triaged by the CAPI team appropriately.
  - This will need named individuals to be able to log in to bugs.chromium.org with a valid Google account, for

Assignees

AdamKorcz

Labels

area/security area/testin sig/security

Projects

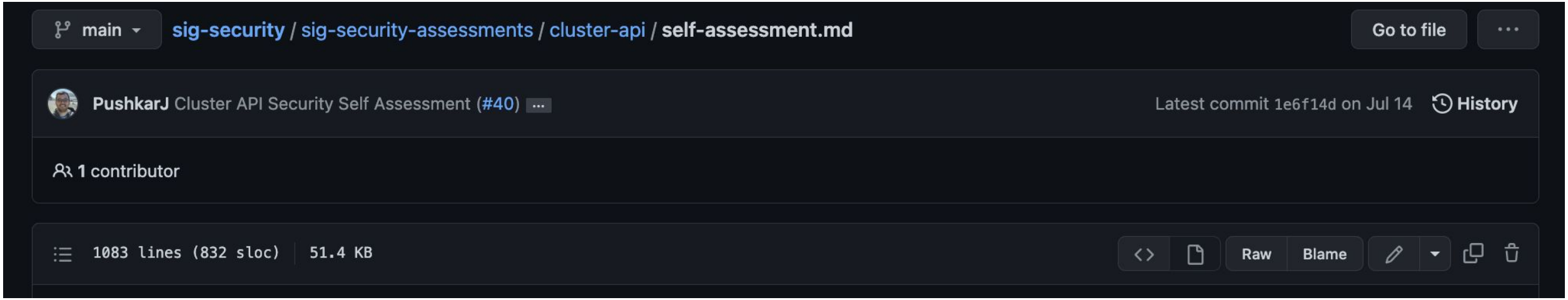
sig-security-tracker

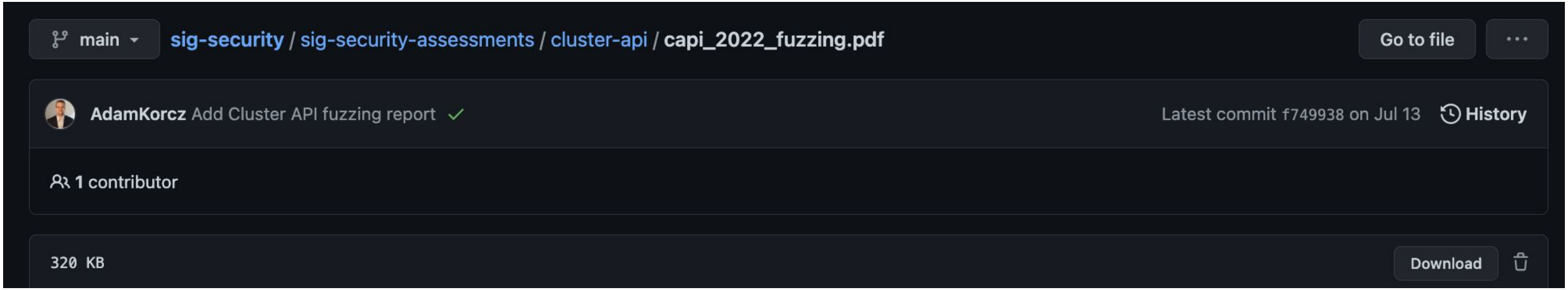
Done

See also: “Fuzzing Session: Finding Bugs and Vulnerabilities Automatically” - David & Adam Korczynski, Ada Logics at 4pm on Friday in Room 260: https://sched.co/1BvfI

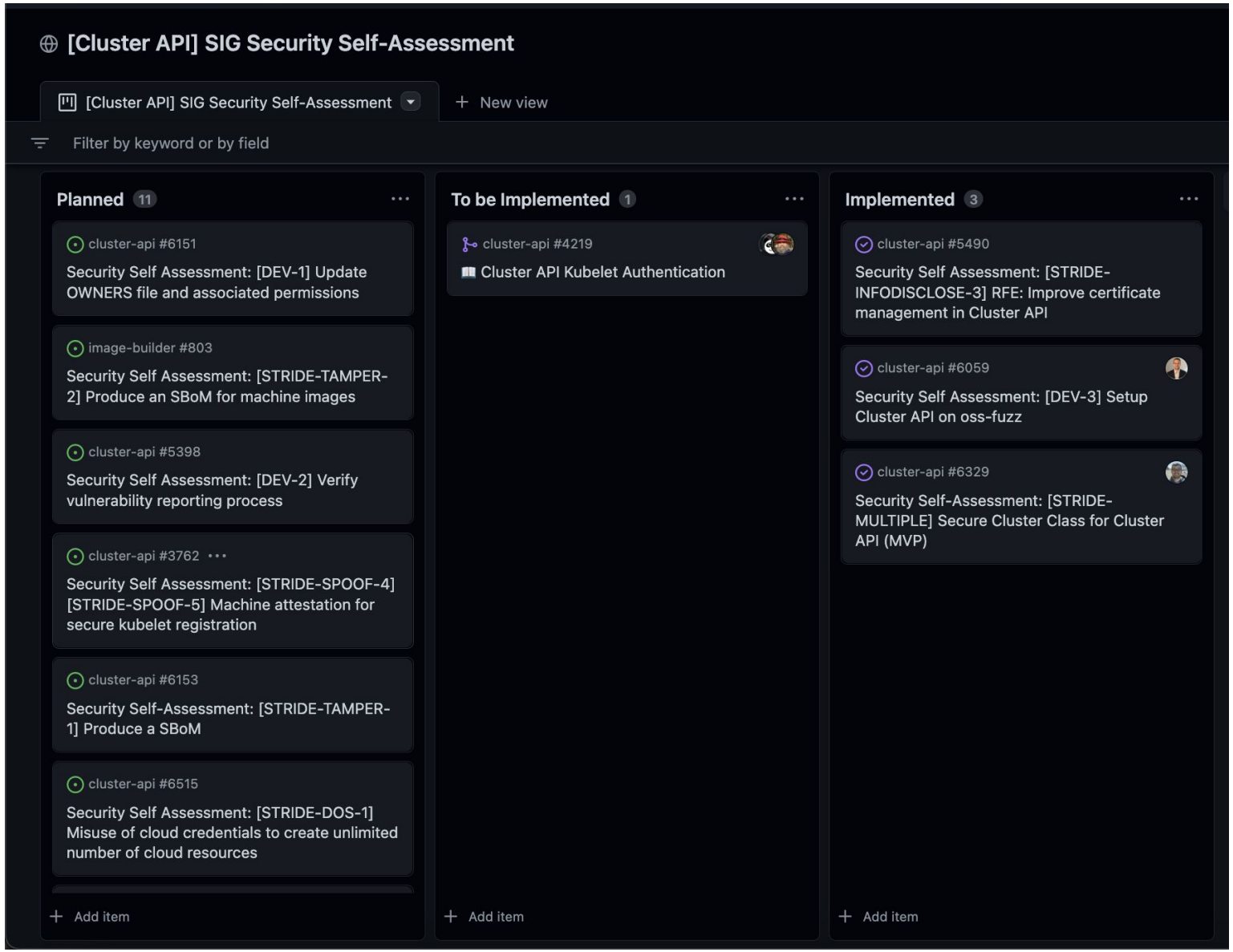
Final outcome

Ref: https://github.com/kubernetes/sig-security/tree/main/sig-security-assessments/cluster-api





What's Next?



Ref: https://github.com/orgs/kubernetes/projects/83/views/1

What's Next?

KubeCon CloudNativeCon North America 2022

Thursday, October 27 • 3:25pm - 4:00pm

Back To Schedule

SIG Security: Empowerment Through Autonomy - Ala Dewberry, VMware; Savitha Raghunathan, Red Hat; Tabitha Sable, Datadog

Sign up or log in to save this to your schedule, view media, leave feedback and see who's attending!

https://sched.co/182(Tweet Share

SIG Security takes a community-building approach to improving Kubernetes security, both for the project itself and our end users. Join organizers Ala, Rey, Savitha, and Tabitha for an overview of how we make space for security collaboration to thrive. We'll share timely updates from our documentation, third-party audit, and tooling subprojects. Security self-assessments will be a special focus, with a deep-dive on this new service offered to Kubernetes by our newest subproject! The Self-Assessments subproject in SIG Security is here to make security introspection accessible to any and all SIGs and subprojects. We aim to give SIGs and subprojects a repeatable and rigorous way to think about their own security, making Kubernetes safer to use as more workloads find their way to it. You'll learn what's been going on, what's next, and how you could join in, regardless of your experience from beginner to expert. We hope to see you there!

BUILDING FOR THE ROAD AHEAD

DETROIT 2022

Q & A

You ask & we try to answer :)

BUILDING FOR THE ROAD AHEAD

DETROIT 2022

Thank you!

See you around :)


KubeCon
CloudNativeCon
North America 2022
BUILDING FOR THE ROAD AHEAD
DETROIT 2022
TiKV
TiKV
HELM

KubeCon | CloudNativeCon
North America 2022

BUILDING FOR THE ROAD AHEAD

DETROIT 2022

Please scan the QR Code above to leave feedback on this session