KubeCon | CloudNativeCon

Europe 2022

WELCOME TO VALENCIA

KubeCon CloudNativeCon Europe 2022

SIG Security Update: We Lift Together

Tabitha Sable, Datadog
Savitha Raghunathan, Red Hat
Rey Lejano, SUSE
Pushkar Joglekar, VMware

SIG Security Update: We Lift Together

Tabitha Sable
Staff Engineer
Datadog

Pushkar Joglekar
Sr. Security Engineer
VMware

Savitha Raghunathan
Sr Software Engineer
Red Hat

Rey Lejano
Field Engineer
SUSE

Who We Are?

- What is SIG Security?
  - Horizontal SIG covering security initiatives for the entire Kubernetes project
- What do we do?
  - Feature, process, and documentation improvements
  - Security-related services within Kubernetes
  - Public forum for Security Response Committee
- How do we do it?
  - Community!
  - Collaboration with sibling SIGs

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

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

Third-Party Security Audit is In-Progress!

Third-Party Security Audit

- Last audit was in 2019
- RFP was released in 2021
- NCC Group was selected to conduct the 2021/2022 audit
- Audit will be based on v1.24.0
- The RFP and RFP Decision are published on GitHub
  - https://github.com/kubernetes/sig-security/tree/main/sig-security-external-audit/security-audit-2021-2022

Third-Party Security Audit

Primary Scope:

- kube-apiserver
- kube-scheduler
- kube-controller-manager
- kubelet
- kube-proxy
- secrets-store-csi-driver

Secondary Scope:

- etcd, Kubernetes use of
- cloud-controller-manager

Third-Party Security Audit

What's Next:

- Publish findings this summer

- Audit Roadmap:
  - Kubernetes is a large project (197 enhancements in the last 4 minor releases)
  - An audit roadmap is designed to guide the focus areas of future audits

Tooling

- Build, Enhance and Improve security through code by working across SIGs and other sub-projects

Tooling

- Create space for new contributors to share and learn
- You can be a speaker too!! Hit this link to add yourself to the list :)

Learning Sessions

Here is the list of learning sessions hosted by sig-security tooling community:

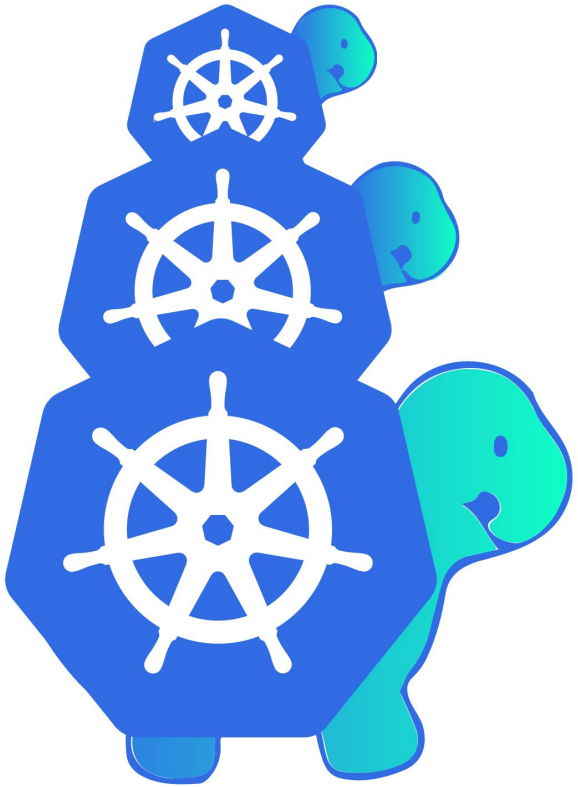
Date	Topic	Speaker	Link
01-18-2022	kdigger	Mahé Tardy	https://www.youtube.com/watch?v=o-E6aoKmznY
11-16-2021	Kube Armor	Rahul Jadhav	https://www.youtube.com/watch?v=MWAb63gf3gs
09-21-2021	SBoM for K8s	Adolfo García Veytia	https://www.youtube.com/watch?v=zB1-7NLsfps
08-17-2021	go-vulncheck	Zvonimir Pavlinovic	https://www.youtube.com/watch?v=YUhiWK15yEc
07-20-2021	Images in k/k discussion	Stephen Augustus	https://www.youtube.com/watch?v=oibVXk9AwO4

Ref: https://github.com/kubernetes/sig-security/blob/main/sig-security-tooling/learning-sessions.md

Security Self-Assessments

Under Review: https://github.com/kubernetes/sig-security/pull/40

CNCF TAG Security + *Kubernetes SIG Security* + *Cluster API*



Logos borrowed from official GitHub Repos

Documentation Deep Dive

- 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:

  - Kubernetes Security Checklist
  - PSP deprecation clean up

Documentation Deep Dive

Blogs

- A Closer Look at NSA/CISA Kubernetes Hardening Guidance
- Securing Admission Controllers
- RBAC Guide
- Cloud native security for your clusters

Documentation Deep Dive

Tutorials & Tasks

- Apply Pod Security Standards at the Cluster Level
- Apply Pod Security Standards at the Namespace Level
- Verify Signed Container Images

Documentation Deep Dive

Papers & Threat Models

- Kubernetes Admission Control Threat Model

- Kubernetes Policy Management

Documentation

- sig-security-docs project is looking for volunteers!
- If you are interested in improving the security content, please feel free to reach out to us in the sig-security-docs slack channel

How You Can Get Involved?

- SIG Meeting: bi-weekly (every other week) 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