CNCF Security SIG
Status: 25 June 2019

Brandon Lum • 25.06.2019
Tuesday, June 25 • 11:45 - 12:20

Overview

Focus areas

- Protection of cloud native* systems, while providing needed access
- Common understanding and common tooling to help developers meet security requirements
- Common tooling for audit and reasoning about system properties.

* cloud native *adj.*

heterogeneous, distributed and fast changing systems

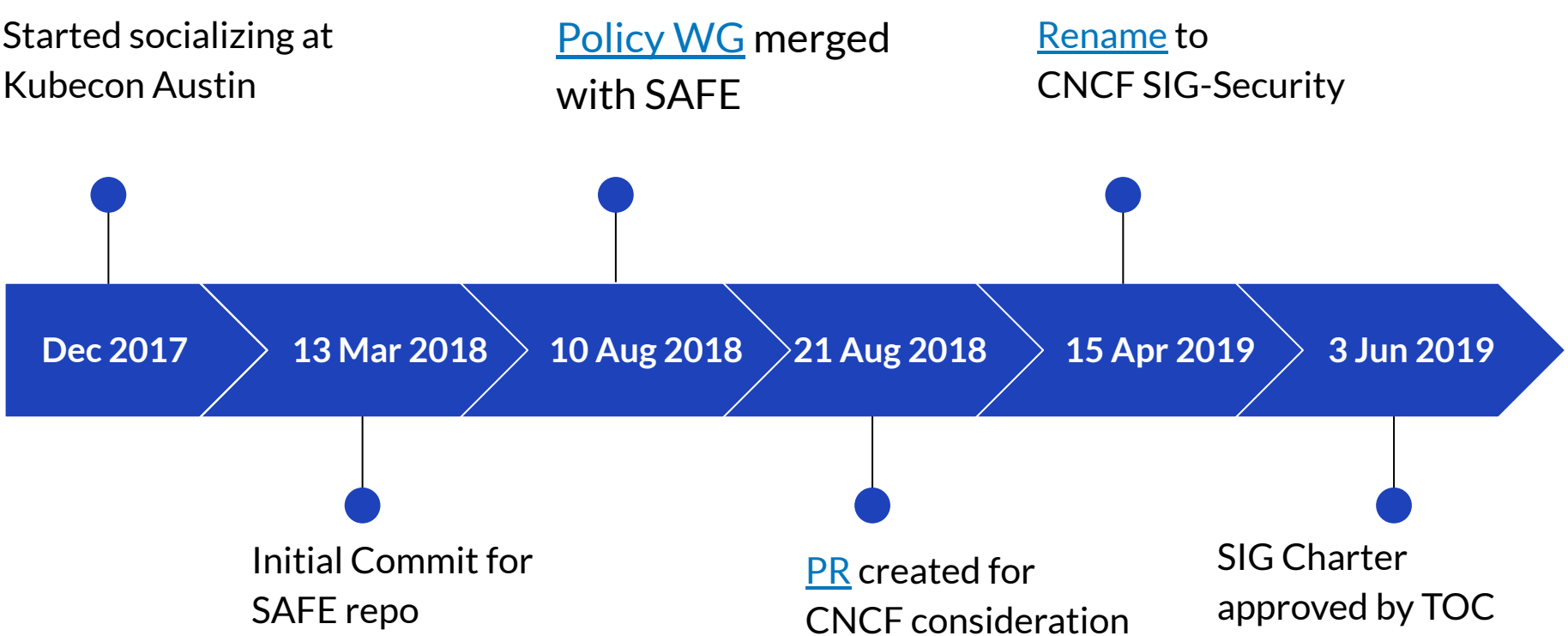
Overview

Focus areas

- Protection of cloud native* systems, while providing needed access
- Common understanding and common tooling to help developers meet security requirements
- Common tooling for audit and reasoning about system properties.

* cloud native *adj.*

heterogeneous, distributed and fast changing systems


Started socializing at Kubecon Austin
Policy WG merged with SAFE
Rename to CNCF SIG-Security
Dec 2017
13 Mar 2018
10 Aug 2018
21 Aug 2018
15 Apr 2019
3 Jun 2019
Initial Commit for SAFE repo
commit fe999bd637456ade5e6cc8866d0db4107a0d9778
Author: Dan Shaw <github@dshaw.com>
Date: Tue Mar 13 18:30:43 2018 -0400
Initial commit
PR created for CNCF consideration
SIG Charter approved by TOC

Members (Current: 44)

- Dan Shaw (@dshaw), PayPal [chair]
- Sarah Allen (@ultrasaurus), [chair]
- Jeyappragash JJ (@pragashj), Tetrate.io [chair]
- Devarajan P Ramaswamy (@deva), PADME
- Kamil Pawlowski (@kbpawlowski)
- Geri Jennings (@izgeri), CyberArk
- Howard Huang (@hannibalhuang), Huawei [Kubernetes Policy WG co-chair]
- Jason Melo (@jasonmelo), NearForm
- Torin Sandall (@tsandall), OPA
- Sree Tummidi (@sreetummidi), Pivotal [Cloud Foundry Project Lead]
- Christian Kemper (@ckemper67), Google
- Ray Colline (@rcolline), Google
- Doug Davis (@duglin), IBM
- Sabree Blackmon (@heavypackets), Docker
- Justin Cormack (@justincormack), Docker
- Liz Rice (@lizrice), Aqua Security
- Erik St. Martin (@erikstmartin), Microsoft
- Cheney Hester (@quiqie), Fifth Third Bank
- Erica von Buelow (@ericavonb), Red Hat [Kubernetes Policy WG]
- Mark Underwood (@knowlengr)
- Rae Wang (@rae42), Google
- Rachel Myers (@rachelmyers), Google
- Evan Gilman (@evan2645), Scytale.io
- Andrew Weiss (@anweiss), Docker
- TK Lala (@tk2929), ZcureZ
- Maor Goldberg (@goldberg10)
- Andrew Martin (@sublimino), ControlPlane
- Karthik Gaekwad (@iteration1), Oracle
- Chase Pettet (@chasemp), Wikimedia Foundation
- Jia Xuan (@xuanjia), China Mobile
- John Morello (@morellonet), Twistlock
- Alban Crequy (@alban), Kinvolk
- Michael Schubert (@schu), Kinvolk
- Andrei Manea (@andrei_821), CloudHero
- Justin Cappos (@JustinCappos), New York University
- Santiago Torres-Arias (@SantiagoTorres), New York University
- Brandon Lum (@lumjjb), IBM
- Ash Narkar (@ashutosh-narkar), OPA
- Lorenzo Fontana (@fntlnz), Sysdig [Falco Maintainer]
- Leonardo Di Donato (@leodido), Sysdig [Falco Maintainer]
- Daniel Iziourov (@danmx), Adevinta
- Michael Hausenblas (@mhausenblas, AWS
- Zach Arnold (@zparnold), Ygrene Energy Fund
- Tsvi Korren (@tsvikorren), Aqua Security

Landscape

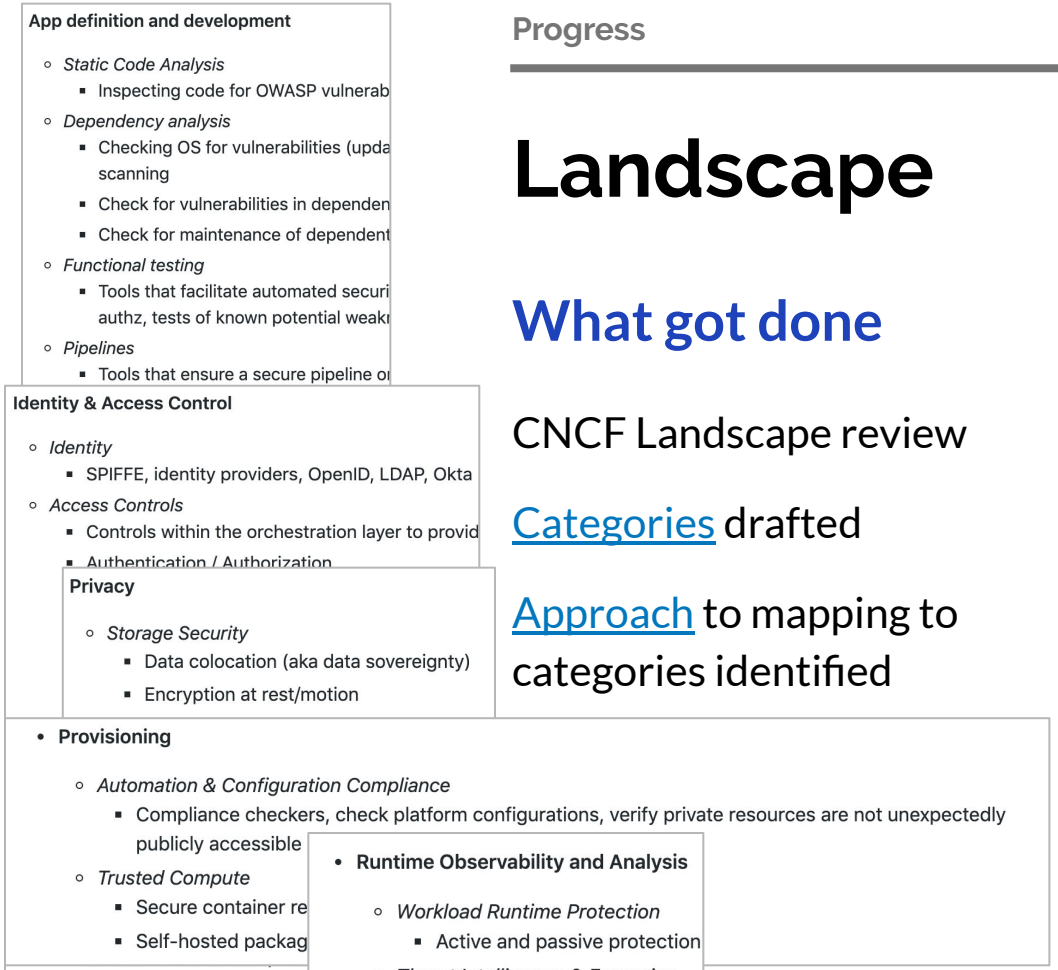
What got done

CNCF Landscape review

Categories drafted

Approach to mapping to categories identified

567 open source projects
40 security-related



Landscape

What got done

CNCF Landscape review

Categories drafted

Approach to mapping to categories identified

Things to do

Validate categories & approach

Map existing projects to categories

Want to help? ⇒ issue#124

Security Assessments

What got done

Initial Guidelines PR#125

Issue Template

KubeCon EU 2019
Inside CNCF Project Security Reviews

sched.co/MPdf

Security Assessments

What got done

Initial Guidelines PR#125

Issue Template

github.com
/cncf/sig-security
/assessments

Almost Completed

In-toto 🤔@SantiagoTorres
Santiago Torres-Arias
Issue#166

OPA 🤔@ashutosh-narkar
Ash Narkar
Issue#179

KubeCon EU 2019
Inside CNCF Project Security Reviews

sched.co/MPdf

Security Assessments

What got done

Initial Guidelines PR#125

Issue Template

Almost Completed

In-toto 🤔@SantiagoTorres
Santiago Torres-Arias

OPA 🤔@ashutosh-narkar
Ash Narkar

Next steps

Expand the security review team…

Want to help? ⇒ shout out on mailing list or slack!

And put your name down in: Issue#167

KubeCon EU 2019
Inside CNCF Project Security Reviews

sched.co/MPdf

Coming up...

2019 Roadmap

- **Security overview White paper** - ***issue#138***
- Policy white paper
- Sig-Security Microsite
- Security assessments
  First 5 - ***issue#167***
  - in-toto
  - OPA
  - Falco
  - Keycloak
  - TBD

learn more...

github.com/cncf/sig-security

Slack: https://slack.cncf.io/ #sig-security

Meeting Times:

Every Wednesdays

10am PT, 1 pm ET, 6pm CET

(zoom: https://zoom.us/my/cncfsigsecurity)