

---

---

# 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.

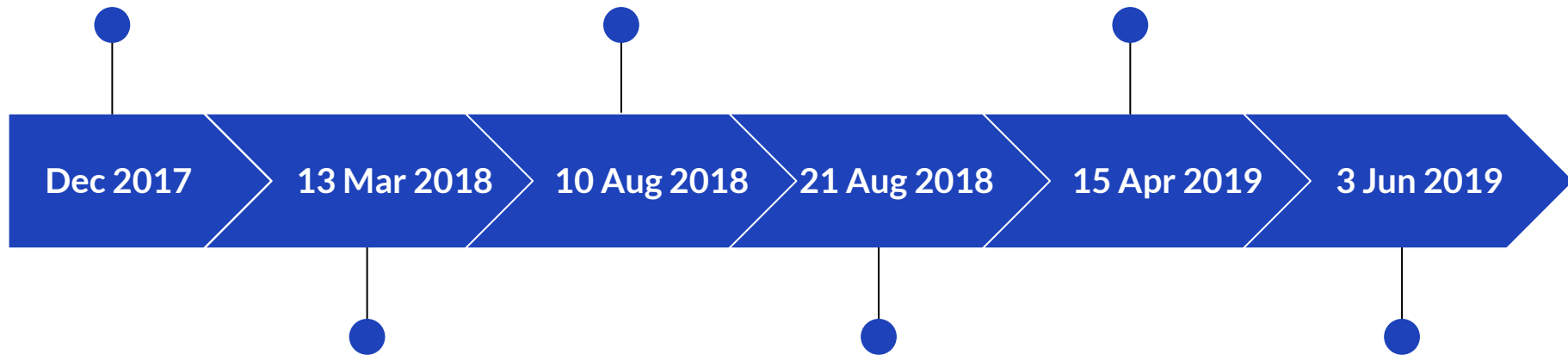
\* cloud native *adj.*

heterogeneous, distributed and fast changing systems

Started socializing at  
Kubecon Austin

[Policy WG](#) merged  
with SAFE

[Rename](#) to  
CNCF SIG-Security



Initial Commit for  
SAFE repo

```
commit fe999bd637456ade5e6cc8866d0db4107a0d9778
Author: Dan Shaw <github@ddshaw.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]
- Jeyappagash JJ ([@pragashi](#)), Tetrade.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 Tummidu ([@sreetummidu](#)), 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 ([@rachellymyers](#)), 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 ([@lumjib](#)), IBM
- Ash Narkar ([@ashutosh-narkar](#)), OPA
- Lorenzo Fontana ([@fntlnz](#)), Sysdig [Falco Maintainer]
- Leonardo Di Donato ([@leodido](#)), Sysdig [Falco Maintainer]
- Daniel Iziourov ([@danmx](#)), Adevinia
- 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*

---

#### App definition and development

- *Static Code Analysis*
  - Inspecting code for OWASP vulnerab
- *Dependency analysis*
  - Checking OS for vulnerabilities (upda scanning
  - Check for vulnerabilities in dependen
  - Check for maintenance of dependent
- *Functional testing*
  - Tools that facilitate automated securi authz, tests of known potential weak
- *Pipelines*
  - Tools that ensure a secure pipeline o

#### Identity & Access Control

- *Identity*
  - SPIFFE, identity providers, OpenID, LDAP, Okta
- *Access Controls*
  - Controls within the orchestration layer to provid
  - Authentication / Authorization

#### Privacy

- *Storage Security*
  - Data colocation (aka data sovereignty)
  - Encryption at rest/motion

#### • Provisioning

- *Automation & Configuration Compliance*
  - Compliance checkers, check platform configurations, verify private resources are not unexpectedly publicly accessible
- *Trusted Compute*
  - Secure container re
  - Self-hosted packag
- Provisioning of SSL certs fo

#### • Runtime Observability and Analysis

- *Workload Runtime Protection*
  - Active and passive protection
- *Threat Intelligence & Forensics*
  - Threat analytics, auditing
- *Defense and Monitoring*

## Progress

---

# 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](https://sched.co/MPdf)

---



# Security Assessments

## What got done

Initial Guidelines [PR#125](#)

github.com  
/cncf/sig-security  
/assessments

Issue Template

## 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](https://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](https://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/](https://slack.cncf.io/#sig-security) #sig-security

**Meeting Times:**

**Every Wednesdays**

10am PT, 1 pm ET, 6pm CET

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