CNCF Security SIG
Status: 19 Nov 2019

Sarah Allen (@ultrasaurus) & Brandon Lum (@lumjjb)

Tuesday, November 19 • 10:55 - 11:30

Who We Are

Things We Do

Get Involved

Who we are

Mission

to reduce risk that cloud native applications expose end user data or allow other unauthorized access.

Charter

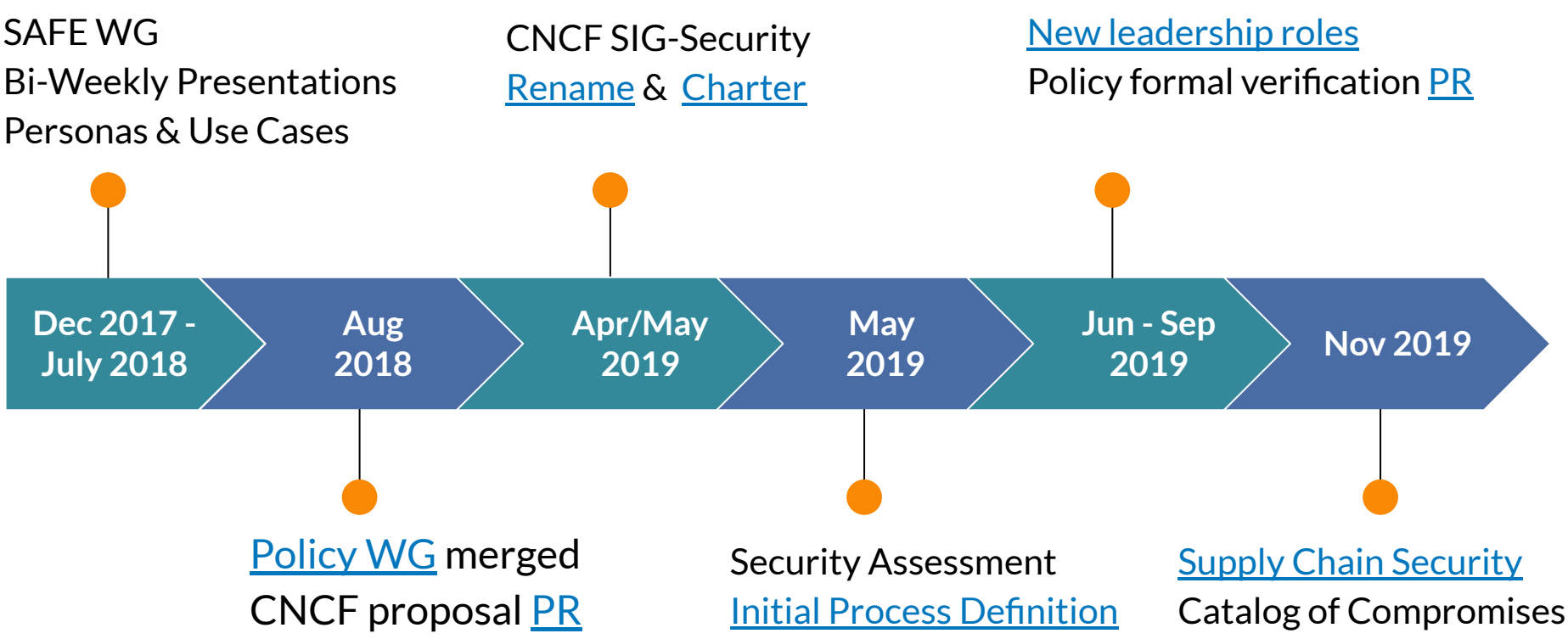
Focus areas

- 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.

Charter

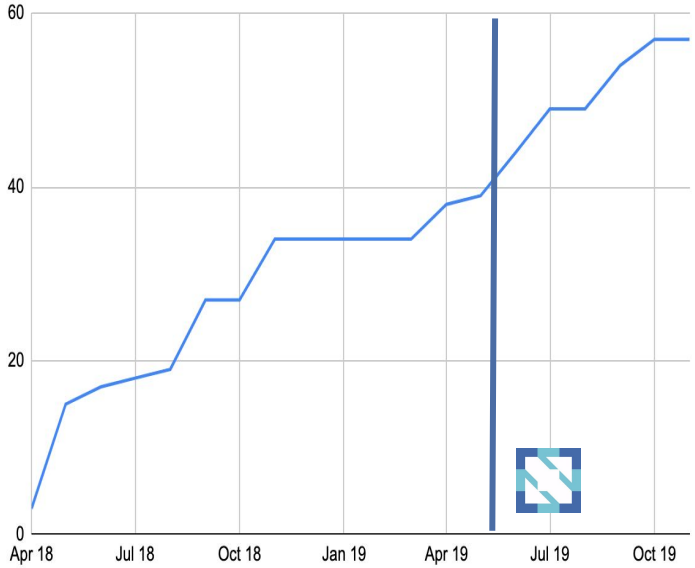
Focus areas

- 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.


SAFE WG
Bi-Weekly Presentations
Personas & Use Cases
CNCF SIG-Security
Rename & Charter
New leadership roles
Policy formal verification PR
Dec 2017 - July 2018
Aug 2018
Apr/May 2019
May 2019
Jun - Sep 2019
Nov 2019
Policy WG merged
CNCF proposal PR
Security Assessment
Initial Process Definition
Supply Chain Security
Catalog of Compromises

Members (Current: 57)

- Dan Shaw (@dshaw), [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
- Jason Melo (@jasonmelo), NearForm
- Torin Sandall (@tsandall), OPA
- Sree Tummidi (@sreetummidi), Pivotal
- 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
- 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
- Simarpreet Singh (@simar7)
- Michael Ducy (@mfdii)
- Craig Ingram (@cji), Salesforce
- Roger Klorese (@qnetter), SUSE
- John Menerick (@cloudsriseup), Ford Autonomic
- Peter Benjamin (@petermbenjamin), Teradata
- Emily Fox(@TheFoxAtWork), National Security Agency, U.S.A.
- Carlos Villavicencio (@solrac901), Intel
- Gareth Rushgrove (@garethr), Snyk
- Martin Vrachev (@MVrachev), VMware
- Ricardo Aravena (@raravena80), Rakuten
- Lakshmi Manohar Velicheti (@manohar9999), Shape Security



Things we do

Things we do

Presentations/Demos

In-Person Meetups

Security Assessments

Community Driven Projects

- Supply Chain Initiative
- CNCF Security Day
- Policy Formal Verification definition & use cases

Interested to propose a topic?

Create an issue!

Presentations & Discussions

Past use-cases:

- Fintech k8s
- CyberArk: Application Identity in Cloud Foundry & K8s

Others:

- K8s Security Review by Trail of Bits
- Falco Security Review Process
- Projects: Kamus, Open Policy Agent, In-toto

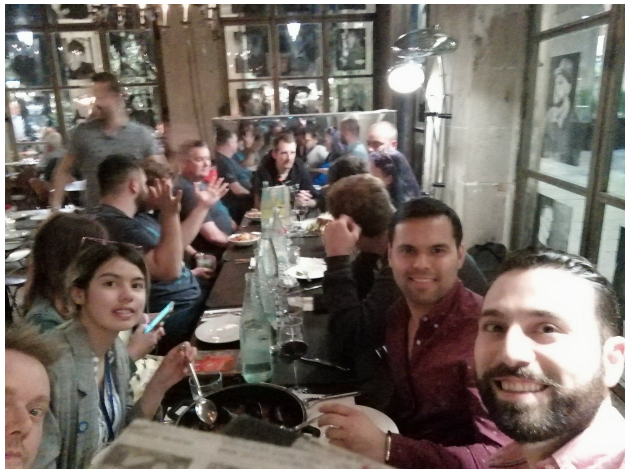
In-Person Meetups

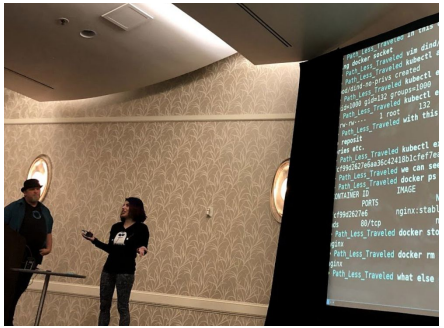
KubeCon + CloudNativeCon San Diego, US, 2019 (#128)
KubeCon + CloudNativeCon Shanghai, CN, 2019 (#200)
KubeCon + CloudNativeCon Barcelona, Spain, 2019 (#127)
DockerCon US 2019 (#151)
...

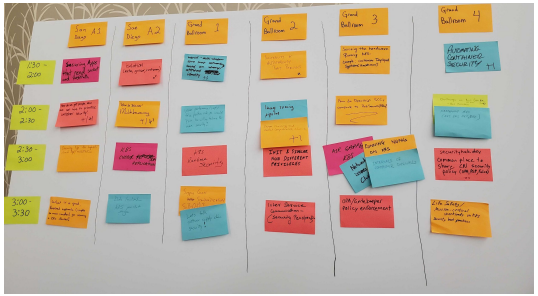
JOIN US TONIGHT!
(#128)

7:15pm

Around Puppy Palooza
(Check issue/twitter)





- 9 Talks
- 

Thank You to our Sponsors

DIAMOND

IBM paloalto NETWORKS Sysdig

PLATINUM

DivvyCloud

GOLD

snyk

github.com/cncf/sig-security #sigsecurity

Security Assessments

Process Overview

- 3 weeks
- Create tracking issue
- Project self-assessment
- Initial Review
- Presentation to sig
- Final Assessment

Interested?

Each requires >2 experienced reviewers (including lead), but additional reviewers are welcome!

Want to help? ⇒ shout out on slack!

Security Assessments

What got done

Project Lead / Review Role

Assessment code-of-conduct (PR#285)

Completed!

In-toto 😃@SantiagoTorres
Santiago Torres-Arias

OPA 😃@ashutosh-narkar
Ash Narkar

What's next?

Security Assessment intake process (PR#281)

github.com /cncf/sig-security /assessments

Landscape

What got done

Improvements:

- Clarify Identity category (#274)
- Add Compliance perspective (#291)

567 open source projects
40 security-related

Personas

What got done

- Platform Implementor Persona (#246)

Platform Implementer

The recognition of the platform implementer as a distinct role is a relatively recent phenomenon. The goal of the platform implementer is to take the business requirements and translate them to the underlying technology or cloud platform to make the organization's **enterprise, network and quota operators** and **security administrators and compliance officers** successful.

One important aspect of this role may be to bridge between the heterogenous cloud environments that are in use at the organization to provide a homogeneous management surface to the administrators and operators. This role is more technical than the roles of the operators and administrators and will often overlap with the role of a developer.

- As a platform implementer I can provide central administration of cloud resources to my **operators and administrators**.
- As a platform implementer I can provide compartmentalization of cloud resources for delegation purposes by **operators and administrators**.
- As a platform implementer I can allow my **operators and administrators** to delegate administration of resources.
- As a platform implementer I can enable my **security administrators** to constrain the behavior of **developers** by setting guardrails.
- As a platform implementer I can enable my **security administrators and compliance officers** to enforce auditing of access policies.
- As a platform implementer I can enable my **security administrators and compliance officers** the auditing of resource access.
- As a platform implementer I can enable my **compliance officers** the setting of audit logging policies for my organization's resources
- As a platform implementer I can enable my **compliance officers** to certify the non-violation of my organization's compliance needs.

Supply Chain Initiative

What is it?

Stemmed from initial review of in-toto

Catalog of Supply Chain compromises

Mitigation techniques (Future work)

Provides

Provide a better understanding of supply chain attacks

Provides a document to educate and promote security for decision makers

Get Involved

with  SIG SECURITY

https://github.com/cncf/sig-security

CNCF Special Interest Group for Security (SIG-Security)

Quick links

- Meeting Information
- Slack Information
- New Members
- Members

https://github.com/cncf/sig-security#new-members

New members are advised to:

- Join the CNCF Slack team, particulary #sig-security channel and introduce yourself.
- Initially go through the following documents in the repository:
  - README.md
  - CODE-OF-CONDUCT.md
  - usecases.md
- Regularly join the Zoom meeting at least for the first couple of months to get yourself up to speed.
- Here are multiple ways to get involved:
  - Join the meeting as advised above and express your area of interests or if you want to work on any specific issue.
  - Express your thoughts or ask questions on an issue you find interesting.
  - Choose an issue where help is needed and comment on it expressing interest.

https://github.com/cncf/sig-security/issues

Presentation
Have something you want to share with the group? Or someone you would like to invite to speak? Propose a presentation for the SIG-Security weekly meetings.

Get started

Proposal
To suggest an idea for a new resource or process that will improve cloud native security that you want to work on (if you have an idea that you don't personally want to work on, make a "suggestion")

Get started

Security Assessment
To request a security assessment or track progress on active assessment

Get started

Suggestion
You have an idea for a new resource or process that will improve cloud native security and you aren't sure if you are the person to work on it or want to get feedback from others to refine the idea

Get started

Learn more...

github.com/cncf/sig-security

Wednesday, November 20 • 5:20pm - 5:55pm

CNCF SIG-Security Deep Dive - Jeyappragash Jeyakeerthi, CNCF SIG-Security & Zhipeng Huang, Huawei

https://sched.co/UafZ

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

Meeting Times:

Every Wednesday

10am PT - General Meeting

4pm PT - Policy sub-group