CNCF Security SIG Status: 21 May 2019

Sarah Allen & Jeyappragash JJ • 21.05.2019
Tuesday, May 21 • 15:55 - 16:30

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

7 May 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

Updated Charter and Governance

Members

- 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]

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

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 f

- **Runtime Observability and Analysis**

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

Security Assessments

What got done

Initial Guidelines [PR#125](PR#125)

Issue Template

Wed, May 22
14:00 - 14:35
*Inside CNCF Project
Security Reviews*

sched.co/MPdf

Security Assessments

What got done

Initial Guidelines [PR#125](PR#125)

Issue Template

github.com
/cncf/sig-security
/assessments

In Progress

In-toto 🤔 @SantiagoTorres
Santiago Torres-Arias

OPA 🤔 @ashutosh-narkar
Ash Narkar

Wed, May 22
14:00 - 14:35
*Inside CNCF Project
Security Reviews*

sched.co/MPdf

Security Assessments

What got done

Initial Guidelines PR#125

Issue Template

In Progress

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!

Wed, May 22
14:00 - 14:35
Inside CNCF Project Security Reviews

sched.co/MPdf

Coming up...

2019 Roadmap

- **Security overview White paper** - *issue#138*

- Policy white paper

- Security assessments First 5 - *issue#167*
  - in-toto
  - OPA
  - Falco
  - Keycloak
  - TBD

learn more...

github.com/cncf/sig-security

Wed, May 22

11:05 - 11:40
Deep Dive: CNCF Security SIG
   Justin Cappos, NYU
   Zhipeng Huang, Huawei
   sched.co/Oscd

14:00 - 14:35
Inside CNCF Project Security Reviews
   Justin Cormack, Docker
   Justin Cappos, NYU
   sched.co/MPdf