An Introduction to Cloud Native Security

Emily Fox (@thefoxatwork) & Brandon Lum (@lumjjb)

Thursday, November 19 • 4:50pm - 5:25pm (CEST)

Introduction

Open Source Projects

Security Resources

Get Involved

Mission

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

Charter

Focus areas

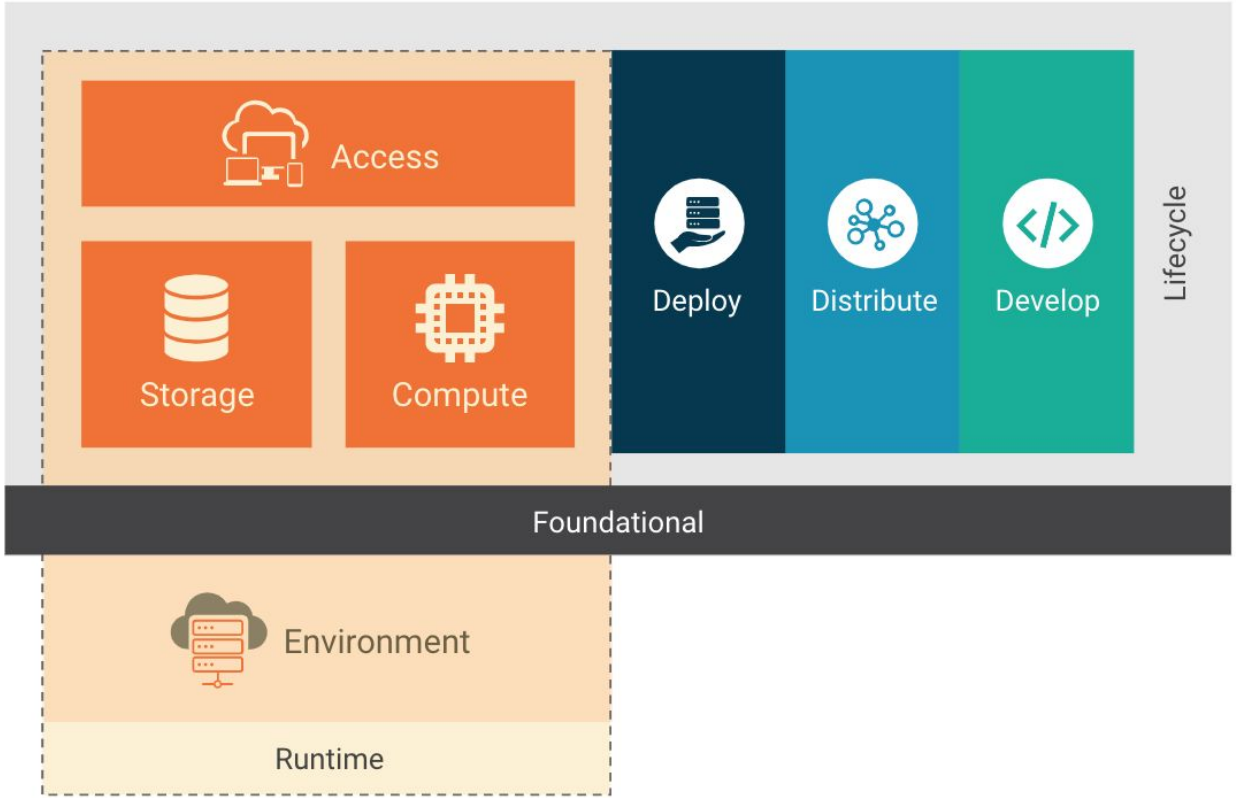
- Protection of cloud native systems, while providing needed access
- Common understanding and common tooling to help developers meet security requirements
- Common tooling for audit and reasoning about system properties.

Open Source Projects

- 36 pages
- Executive summary
- My first secure cloud native architecture
- Everything to get started in a secure cloud native workload
- Landscape companion
- Cloud Native Security Layers

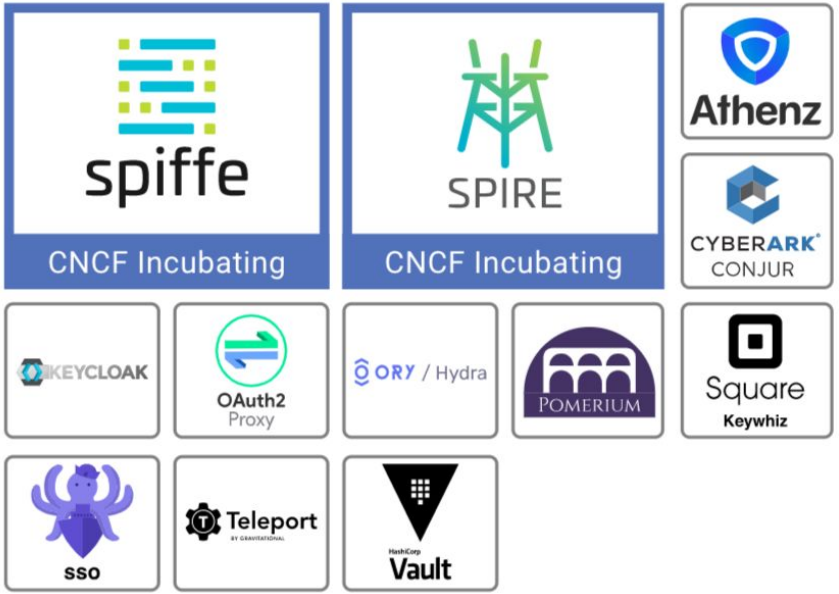
Cloud Native Security Whitepaper

Cloud native security layers



Container Registry

Key Management



https://landscape.cncf.io/

Security & Compliance

https://landscape.cncf.io/

Security Resources & Activities

Interested to propose a topic?

Create an issue!

Presentations & Discussions

Presentations for related projects and groups: K8s security, K8s SIG-Auth, NIST Big Data WG, open source community and projects

Examples:

- PARSEC: Platform AbstRaction for SECurity
- Keylime: Scalable Trust System harnessing TPM
- K8s threat modeling & open source security training
- Discussion: Confidential Computing Consortium

What is it?

Stemmed from initial review of in-toto

Catalog of Supply Chain compromises

Provides

Provides a document to educate and promote security for decision makers

Supply Chain Catalog

(/cncf/sig-security/supply-chain-security/)

This repository contains links to articles of software supply chain compromises. The goal is not to catalog every known supply chain attack, but rather to capture many examples of different kinds of attack, so that we can better understand the patterns and develop best practices and tools.

For definitions of each compromise type, please check out our compromise definitions page

We welcome additions to this catalog by filing an issue or github pull request

Name	Year	Type of compromise	Link
Webmin backdoor	2019	Dev Tooling	1, 2
purescript-npm	2019	Source Code Compromise	1 and 2
electron-native-notify	2019	Source Code Compromise	1, 2
ShadowHammer	2019	Multiple steps	1, 2
PEAR Breach	2019	Publishing Infrastructure	1, 2
Dofoil	2018	Publishing Infrastructure	1
Operation Red	2018	Publishing Infrastructure	1
Gentoo Incident	2018	Source Code	1
Unnamed Maker	2018	Publishing Infrastructure	1
Colourama	2018	Negligence	1, 2
Foxif/CCleaner	2017	Publishing Infrastructure	1

Community managed catalog!

Come collaborate!

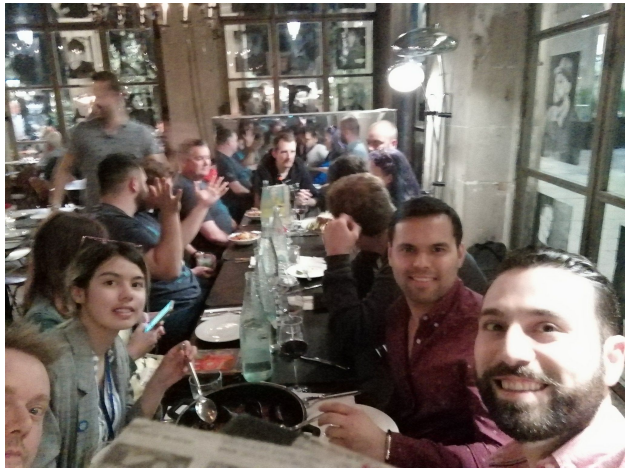
Want to create a meetup?

Create an **issue** with the **event** you are attending and *raise it at the next meeting*!

In-Person Meetups!

We miss you 2019!! 😢

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



Security Assessments

Completed Assessments:

Harbor 

SPIFFE/SPIRE 

In-toto 

OPA 

Keycloak 

- *The security assessment process:*
  1. *Assesses the security posture of a project*
  2. *Informs the CNCF TOC on security aspects of projects*
  3. *Creates a security document for the project*

- Project documents serve as entry points for End User Community adoption of open source projects
  github.com/cncf/sig-security/assessments/projects

Let’s look at an assessment

https://github.com/cncf/sig-security/blob/master/assessments/projects/harbor/self-assessment.md

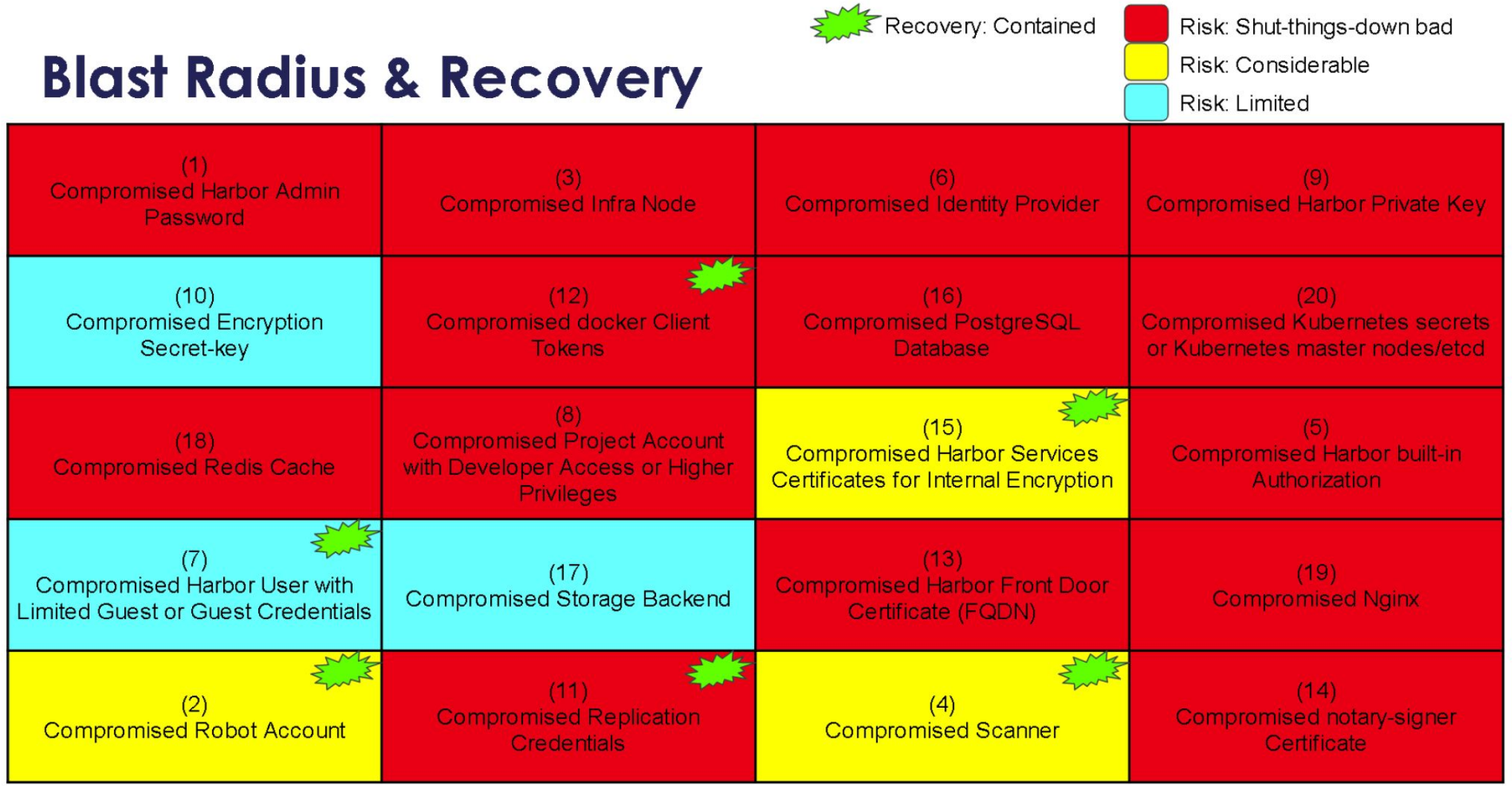
CNCF SIG-Security Harbor Project Self Assessment

March 2020
Primary Author: Michael Michael, Harbor Maintainer (@michmike, @michmike77)
Security Reviewers: Andres Vega, Justin Cappos, Chase Pettet, Vinay Venkataraghavan, Robert Ficaglia, Martin Vrachev, Payam Tarverdyan Chychi, Cameron Seader.

This document details the design goals and security implications of Harbor to aid in the security assessment by CNCF SIG-Security.

Blast Radius Index

Blast Radius & Recovery



Ecosystem

Please see the Goals section at the beginning of this document to understand how Harbor aligns with the cloud native ecosystem.

Security Issue Resolution

Responsible Disclosures Process

Harbor has a comprehensive vulnerability and security policy that is outlined at https://github.com/goharbor/harbor/security/policy. We have already battle tested this policy and our Incident Response more than a few times and it has worked very well for both the Harbor team, our users, as well as the security researchers that reported vulnerabilities and attack vectors. You can view our published advisories at https://github.com/goharbor/harbor/security/advisories?state=published.

Our policy states that anyone who finds a vulnerability should report it to the Harbor security team through cncf-harbor-security@lists.cncf.io with the details of the vulnerability. The email will be fielded by the Harbor Security Team, which is made up of Harbor maintainers who have committer and release permissions. Emails will be addressed within 3 business days, including a detailed plan to investigate the issue and any potential workarounds to perform in the meantime.

Incident Response

If a vulnerability is acknowledged and the timeline for a fix is determined, the Security Team will work on a plan to communicate with the appropriate community, including identifying mitigating steps that affected users can take to protect themselves until the fix is rolled out. The Security Team will also create a CVSS using the CVSS Calculator. The Security Team makes the final call on the calculated CVSS; it is better to move quickly than making the CVSS perfect. The CVE will initially be set to private and Security Team will provide early disclosure of the vulnerability by emailing the cncf-harbor-distributors-announce@lists.cncf.io mailing list. A public disclosure date is then negotiated by the Harbor Security Team, the bug submitter, and the distributors list. Once the fix is confirmed, the Security Team will patch the vulnerability in the next patch or minor release, and backport a patch release into all earlier supported releases.

OPA: Policy-based control for cloud native environments

Goal: provide consistent policy enforcement.

Design: General-purpose policy engine to enforce custom policies in disparate systems using a high-level declarative language ("Rego").

Security Analysis: benefit for adopters who have heterogeneous infrastructure or high rate of change where lack of policy enforcement would present significant business risk. OPA reduces risk by:

- isolating policy from other business logic
- increasing visibility across the system

Maturity: The core technology is in production with a broad set of companies, incl. Netflix, Cloudflare, Chef. Contributions mostly from Styra, wide community participation (78 contributors).

The added complexity of OPA is not trivial. OPA enables "policy as code" and Rego policy expressions require the same care to develop as any security critical code.

CNCF Recommendations:

- Study of user practices with OPA policies (detect common patterns of insecurity, suggest improvements)
- Collect information from CNCF End User companies that integrate OPA into software and recommend integrations where OPA would have the largest security benefit for the cost.

Project recommendations:

- Improve documentation (common scenarios, deployment)
- Rego usability: reduce errors (testing, playground), increase understanding of security implication
- Expand security response team across companies

github.com/cncf/sig-security/assessments/projects/opa

about security assessments

 Andres Vega

 Ashutosh Narkar

 Brandon Lum

 Cameron Seader

 Chase Pettet

 Emily Fox

 Justin Cappos

 Justin Cormack

 Krishan-Sharma

 Martin Vrachev

 Matt Hamilton

 Payam Tarverdyan Chychi

 Robert Ficaglia

 Sarah Allen

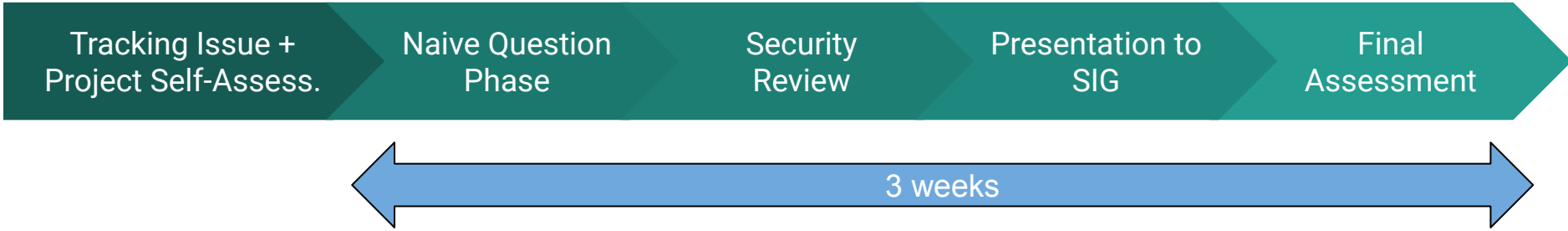
 Vinay Venkataraghavan

Our Reviewers!

Reviewers get the opportunity to:

- Have a deep-dive on new CNCF projects
- Networking with other security reviewers, project members and CNCF staff

Security Assessments



Join a review!

Reviews are sized be done in short sprints and our review team is very friendly!

Want to help? ⇒ shout out on slack! #sig-security
Upcoming assessment: Cloud Native Buildpacks (issue #377)

Get Involved

with

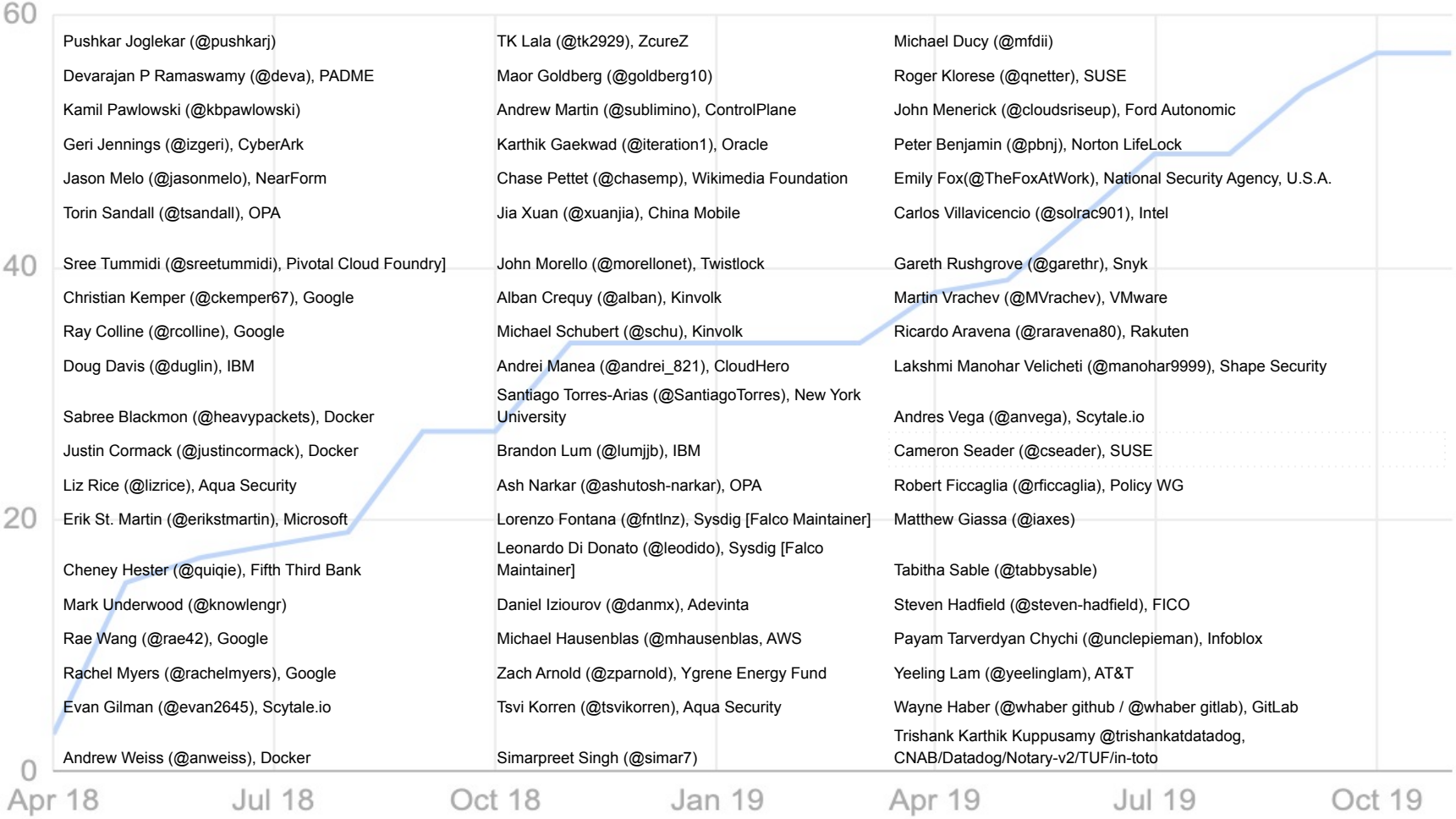
https://github.com/cncf/sig-security

CNCF Special Interest Group for Security (SIG-Security)

Quick links

- Meeting Information
- Slack Information
- New Members
- Members

Members: (Current: 68)



Pushkar Joglekar (@pushkarj)	TK Lala (@tk2929), ZcureZ	Michael Ducy (@mfdii)
Devarajan P Ramaswamy (@deva), PADME	Maor Goldberg (@goldberg10)	Roger Klorese (@qnetter), SUSE
Kamil Pawlowski (@kbpawlowski)	Andrew Martin (@sublimino), ControlPlane	John Menerick (@cloudsriseup), Ford Autonomic
Geri Jennings (@izgeri), CyberArk	Karthik Gaekwad (@iteration1), Oracle	Peter Benjamin (@pbnj), Norton LifeLock
Jason Melo (@jasonmelo), NearForm	Chase Pettet (@chasemp), Wikimedia Foundation	Emily Fox(@TheFoxAtWork), National Security Agency, U.S.A.
Torin Sandall (@tsandall), OPA	Jia Xuan (@xuanjia), China Mobile	Carlos Villavicencio (@solrac901), Intel
Sree Tummidi (@sreetummidi), Pivotal Cloud Foundry]	John Morello (@morellonet), Twistlock	Gareth Rushgrove (@garethr), Snyk
Christian Kemper (@ckemper67), Google	Alban Crequy (@alban), Kinvolk	Martin Vrachev (@MVrachev), VMware
Ray Colline (@rcolline), Google	Michael Schubert (@schu), Kinvolk	Ricardo Aravena (@raravena80), Rakuten
Doug Davis (@duglin), IBM	Andrei Manea (@andrei_821), CloudHero	Lakshmi Manohar Velicheti (@manohar9999), Shape Security
Sabree Blackmon (@heavypackets), Docker	Santiago Torres-Arias (@SantiagoTorres), New York University	Andres Vega (@anvega), Scytale.io
Justin Cormack (@justincormack), Docker	Brandon Lum (@lumjjb), IBM	Cameron Seader (@cseader), SUSE
Liz Rice (@lizrice), Aqua Security	Ash Narkar (@ashutosh-narkar), OPA	Robert Ficcaglia (@rficcaglia), Policy WG
Erik St. Martin (@erikstmartin), Microsoft	Lorenzo Fontana (@fntlnz), Sysdig [Falco Maintainer]	Matthew Giassa (@iaxes)
Cheney Hester (@quiqie), Fifth Third Bank	Leonardo Di Donato (@leodido), Sysdig [Falco Maintainer]	Tabitha Sable (@tabbysable)
Mark Underwood (@knowlengr)	Daniel Iziourov (@danmx), Adevinta	Steven Hadfield (@steven-hadfield), FICO
Rae Wang (@rae42), Google	Michael Hausenblas (@mhausenblas, AWS	Payam Tarverdyan Chychi (@unclepieman), Infoblox
Rachel Myers (@rachelmyers), Google	Zach Arnold (@zparnold), Ygrene Energy Fund	Yeeling Lam (@yeelinglam), AT&T
Evan Gilman (@evan2645), Scytale.io	Tsvi Korren (@tsvikorren), Aqua Security	Wayne Haber (@whaber github / @whaber gitlab), GitLab
Andrew Weiss (@anweiss), Docker	Simarpreet Singh (@simar7)	Trishank Karthik Kuppusamy @trishankatdatadog, CNAB/Datadog/Notary-v2/TUF/in-toto

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

Don't see your issue here? Open a blank issue.

Edit templates

Learn more...

github.com/cncf/sig-security

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

Meeting Times on Wednesdays:

General Meeting: 10am PT every Wednesday

Policy sub-group: 3p PT (bi-weekly)

Sign up for our email list!

https://lists.cncf.io/g/cncf-sig-security/