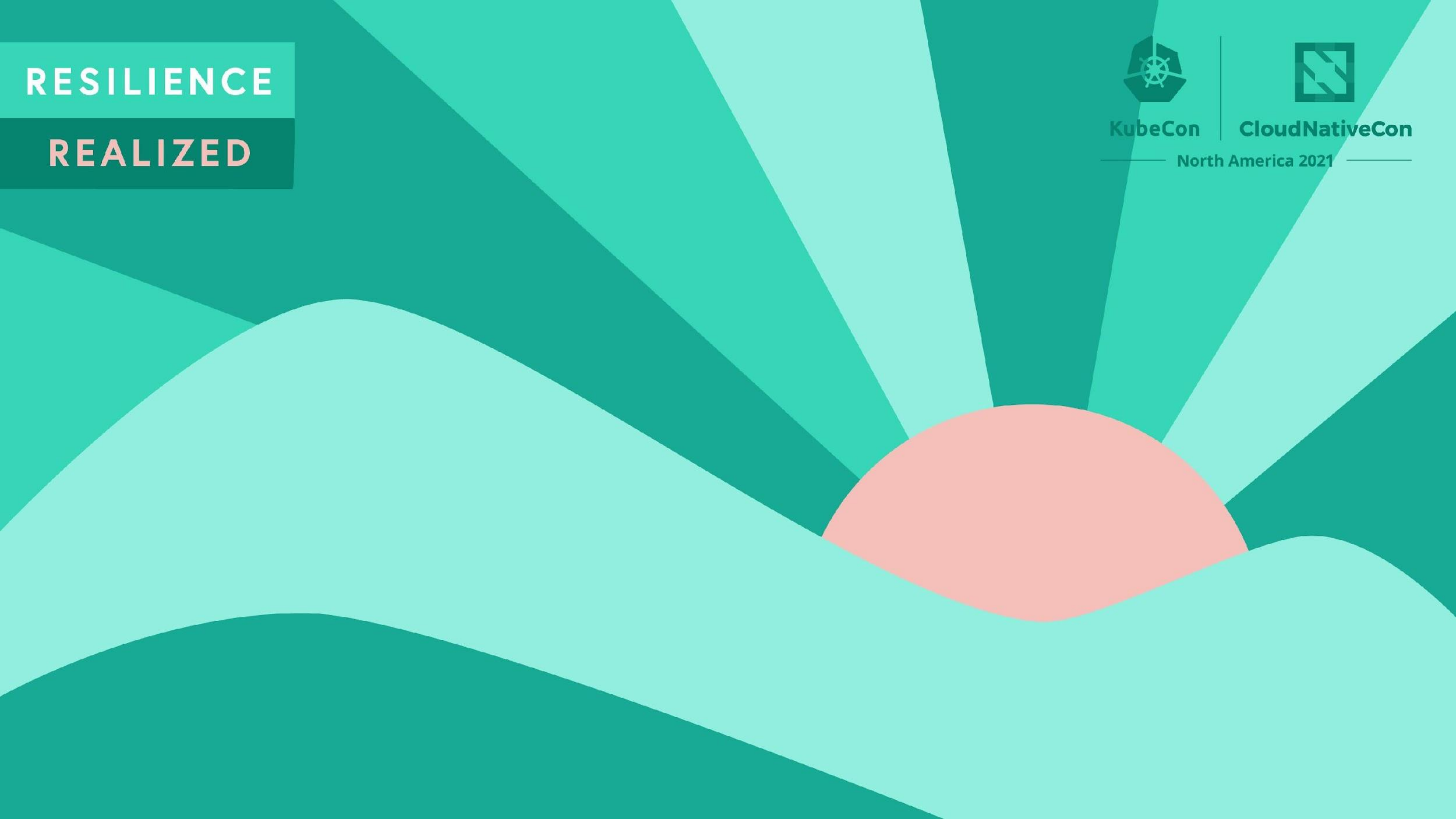


RESILIENCE

REALIZED

KubeCon | CloudNativeCon

North America 2021

KubeCon | CloudNativeCon

North America 2021

RESILIENCE

REALIZED

# Creating Cloud Native Security

*Andrés Vega, VMware & CNCF Security TAG Tech Lead*
*Brandon Lum, IBM & CNCF Security TAG Co-Chair*
*Emily Fox, Apple & CNCF Security TAG Co-Chair*

github.com/CNCF/tag-security

CLOUD
NATIVE
SECURITY

# Security

## Technical Advisory Group

(Security TAG)

github.com/CNCF/tag-security

- Who we are
- What we do
- How is this creating cloud native security?
- Where to jump in

CLOUD
NATIVE
SECURITY

🦝 **Who we are**

What we do

How is this creating cloud native security?

Where to jump in

github.com/CNCF/tag-security

CLOUD
NATIVE
SECURITY

# Security TAG

- What is a Technical Advisory Group?
  - Strengthen the ecosystem
  - Identify Gaps
  - Educate
  - Foster maturity
  - Engage more communities
  - Nurture growth and participation

- Our [Charter] — we focus on
  - **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**

- Enthusiasts, professionals, students, researchers, hobbyists

- More than **90** of us from over 50 companies and organizations!

github.com/CNCF/tag-security

CLOUD
NATIVE
SECURITY

Who we are

**What we do**

How is this creating cloud native security?

Where to jump in

github.com/CNCF/tag-security

CLOUD
NATIVE
SECURITY

# Creating & Breaking

- **Papers**
    - Cloud Native Security Whitepaper v1 2020
    - Supply Chain Security Paper v1 2021
    - Serverless Security Paper *in progress*
    - Policy Paper *in progress*
    - Supply Chain Secure Software Factory Ref. Arch. *in progress*

- **Security Resources**
    - Security Documents templates - SECURITY.md, embargo policy, etc.
    - Cloud Native Security Map
    - Cloud Native Security Lexicon
    - Cloud Native Security Personas
    - Supply Chain Catalog
    - *more in repo!*

github.com/CNCF/tag-security

CLOUD
NATIVE
SECURITY

# Creating & Breaking

## *In Focus: Cloud Native Security Whitepaper*

- Whitepaper detailing what is Cloud Native Security and the various aspects
    - https://github.com/cncf/tag-security/tree/main/security-whitepaper
- **Topics:**
    - Develop, Distribute, Deploy, Runtime
    - Security Assurance
    - Compliance
- **Available translations:**
    - Simplified Chinese
    - Brazilian Portuguese - in progress (#509)
    - Spanish - in progress (#576)
    - *We would love to have more!*

# Creating & Breaking

## *In Focus: Cloud Native Security Map*

- **Cloud Native Security Map**
  - Provide a mapping of CNCF and open source projects to areas of CN Security whitepaper
  - Provide a practical viewpoint and information on topics in the CN Security whitepaper
  - Identify gaps in CN Security in the ecosystem and make recommendations to TOC
- **Cloud Native Security Map v1**
  - Web resource to navigate whitepaper with related projects and resources
  - Add link to website and screenshot
- **Cloud Native Security Map v2 - Guided tours (#737)**
  - guide users from one aspect of cloud-native security to the next path in their cloud-native journey

# Creating & Breaking

KubeCon CloudNativeCon North America 2021

## What is it?

Stemmed from initial review of in-toto

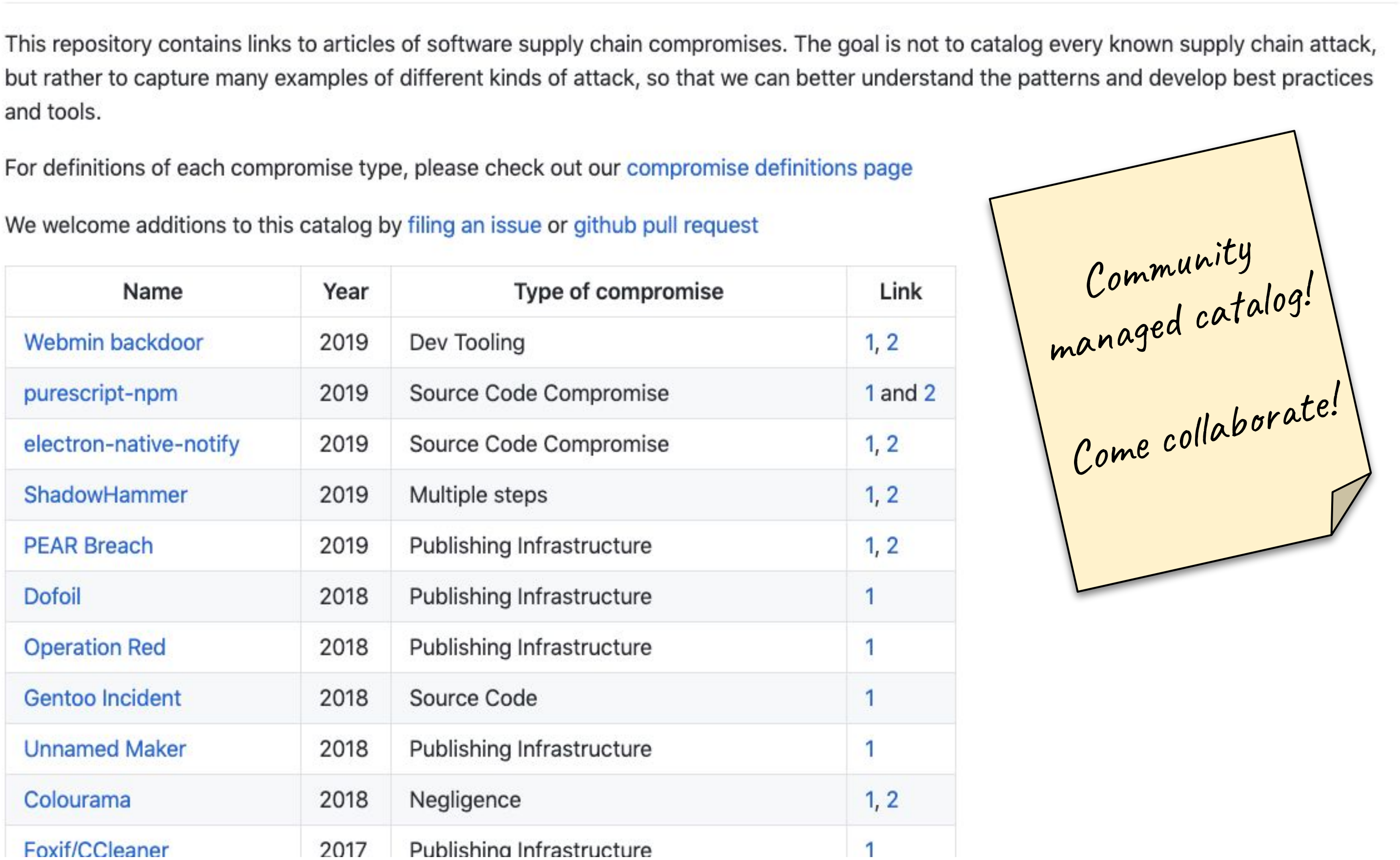
Catalog of Supply Chain compromises

## Provides

Provides a document to educate and promote security for decision makers

# Supply Chain Catalog

(/cncf/tag-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!

github.com/CNCF/tag-security

CLOUD NATIVE SECURITY

Who we are

What we do

**How is this creating cloud native security?**

Where to jump in

github.com/CNCF/tag-security

CLOUD
NATIVE
SECURITY

# Awareness through effort

- Engagement with CNCF & projects results in better security for everyone
  - Security Pals
  - Self-assessment
  - Joint Reviews
  - CKS contribution

- Collaboration with related groups
  - k8s policy working group
  - k8s sig-security
  - Cloud Security Alliance
  - OpenSSF SLSA

- Presentations increase awareness of open source security challenges, solutions, and futures
  - Security focused project presentations
    - Kyverno Overview and Demo
    - Keylime: Scalable Trust System harnessing TPM
  - Security design
    - Security: The selfish interest
  - Calls for action & Resources
    - K8s threat modeling & open source security training

# Awareness through effort

## *In Focus: Security Reviews*

**Security Pals** help projects dip their toe into cloud native security

- friendly face
- security resource

**Self-Assessment** is a resource for sandbox and incubation projects to jump-start their project's security and get them in a better security posture at their own pace

- Security functions & features of project
- Secure development practices, CII badging awareness
- Security issues

**Joint-review** is a collaborative process with Security TAG to perform a table top security review of incubation projects seeking graduation

- Design & configuration
- Attackers, motivations, and threat model
- Hands-on review optional (subject volunteer availability)

*All of these together help projects prepare for a Security Audit!*

github.com/CNCF/tag-security

CLOUD
NATIVE
SECURITY

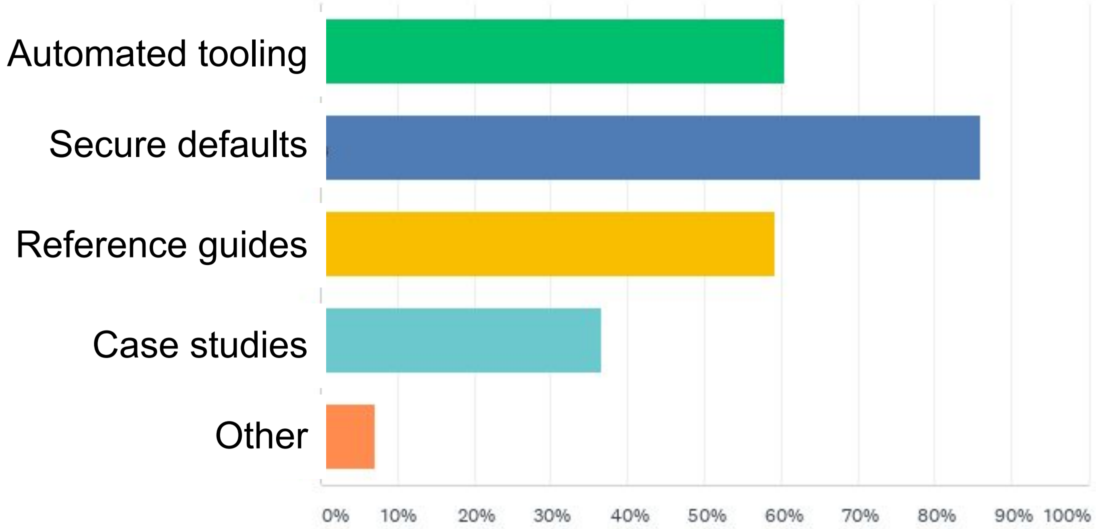
# Awareness through effort

## *In Focus: Cloud Native Security Surveys*

Feedback from surveys drives impact, quality, focus of work

- [Cloud Native Security Whitepaper Retrospective]()
- [Cloud Native Security Microsurvey]()

**What would you like the cloud native security community to focus on?**



Who we are

What we do

How is this creating cloud native security?

**Where to jump in**

github.com/CNCF/tag-security

CLOUD
NATIVE
SECURITY

# One of us! One of us!

- CNCF Security TAG Mailing List → https://lists.cncf.io/g/cncf-tag-security/topics
- Check out good first issue help wanted issues → https://github.com/cncf/tag-security/issues
- Join a meeting → Weekly on Wednesdays at 10:00am UTC-7 via Zoom
- Chat us in Slack → https://cloud-native.slack.com/archives/CDJ7MLT8S #tag-security

R. Raccoon thanks you for attending!

github.com/CNCF/tag-security

CLOUD
NATIVE
SECURITY