CLOUDNATIVE SECURITYCON

NORTH AMERICA 2023

CLOUDNATIVE
SECURITYCON
NORTH AMERICA 2023

TAG Security Cloud Native Security Whitepapers Overview

Shlomo Heigh *Senior Software Engineer, CyberArk*

About me

Shlomo Zalman Heigh

Senior Software Engineer, CyberArk

CYBERARK | Conjur Secrets Manager
Open Source

Developer

- Conjur - open source secrets manager
- Community engagement
- OWASP contributor

Hobbies

- 3D printing
- Woodworking
- RC planes

Social

- LinkedIn.com/in/szheigh
- GitHub.com/szh

A Cloud Native family

C
py had some unusual interests– she was really into genetics and sheep. And so she asked the captain, "Wha
nt to clone myself... On demand... Any number of times?"
" said the captain as he introduced her to Replicaliens.

The Illustrated Children's Guide to Kubernetes

Check out Phippy.io

TAG Security

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

TAG Security

- **1.6k** Github Stars, **384** forks: https://github.com/cncf/tag-security

- Enthusiasts, professionals, students, researchers, hobbyists

- Our role
  - **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**

The Leadership Team

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

Co-chairs

Andrew Martin

Aradhna Chetal

Brandon Lum

Active Tech Leads

Andres Vega

Ashutosh Narkar

Pushkar Joglekar

Justin Cappos

Michael Lieberman

Marina Moore

Ragashree Shekar

Security Assessment Facilitator

Matthew Giassa

TAG Security

Who we are

🦝 What we do

How is this creating cloud native security?

Where to jump in

Creating & Breaking!

Cloud Native Security Whitepaper 2.0

Supply chains security whitepaper

Cloud Native Security Controls catalog

Cloud Native Security Whitepaper Audio release

Whitepapers & Publications

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

TAG SECURITY

CLOUD NATIVE SECURITY WHITEPAPER

VERSION 2

Contributors: Brandon Krieger, Cole Kennedy (TestifySec), Fatih Değirmenci (Ericsson Software Technology), Frederick Kautz , Joel Bork, Marina Moore (NYU), Mateusz Pruchniak, Pushkar Joglekar (VMware), Raja Faisal, Savitha Raghunathan (Red Hat), Sayantani Saha

Reviewers: @jonzeolla, @nyrahul (Accuknox), Ragashree Shekar, Steven Hadfield, Kapil Bareja, Malini Bhandaru, Mikko Ylinen, Jonah Kowall (@jkowall), Kuang Dahu,Ariel Shuper, Eric Li (AlibabaCloud), Tanner Randolph (Applied Systems), Mark Dalton Gray (Microsoft), Ciara Carey, Brandon Lum (TAG Security Chair), Emily Fox (TOC Liaison) and Justin Cormack (TOC liaison)

CLOUD NATIVE COMPUTING FOUNDATION

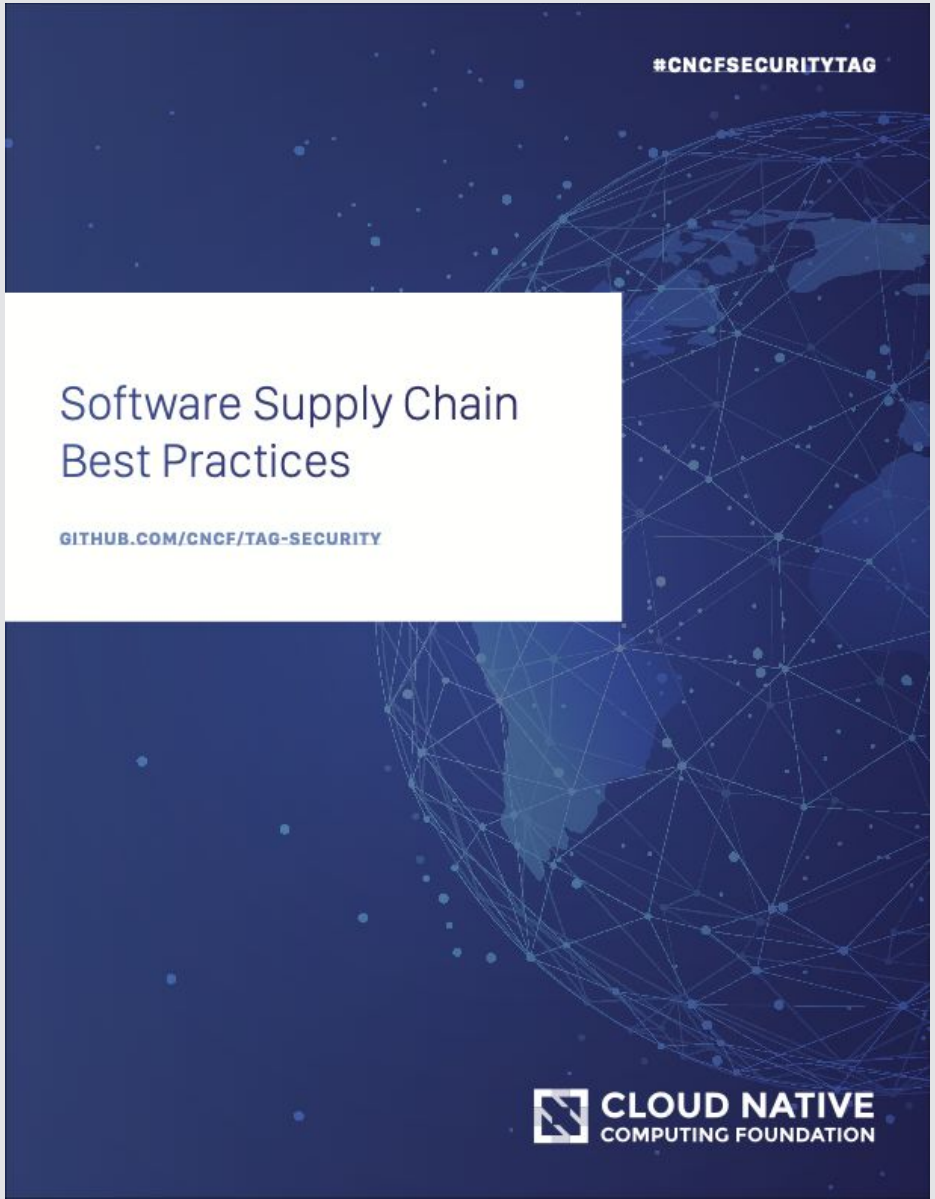
- Markdown
- PDF
- Audio

- Translations in Portuguese and Chinese, plus Italian in progress (issue #1014)

How can you help?

- Contribute to the upcoming v3!
- Record audio of changes

Whitepapers & Publications

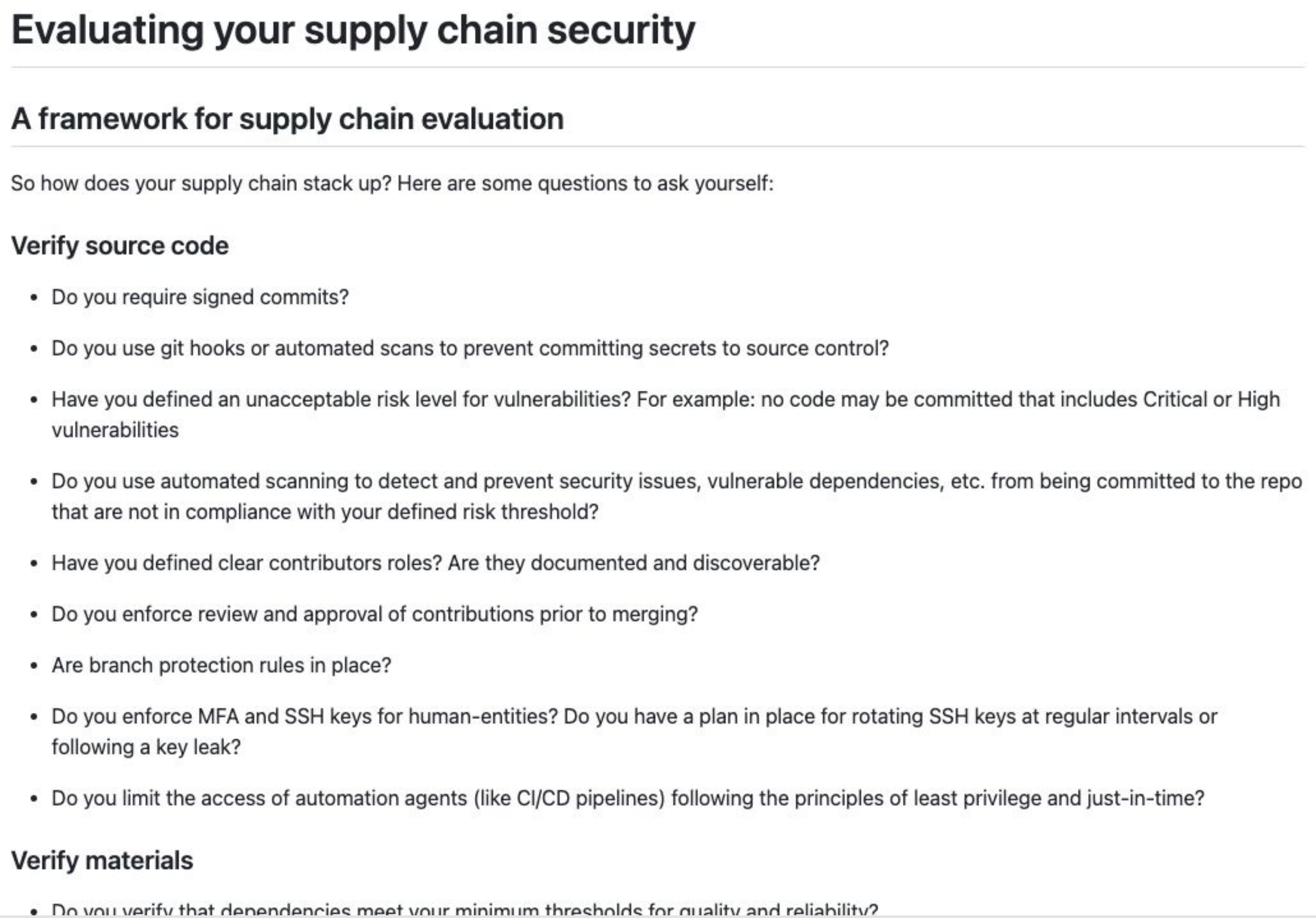


#CNCFSECURITYTAG

Software Supply Chain Best Practices

GITHUB.COM/CNCF/TAG-SECURITY

CLOUD NATIVE COMPUTING FOUNDATION



Evaluating your supply chain security

A framework for supply chain evaluation

So how does your supply chain stack up? Here are some questions to ask yourself:

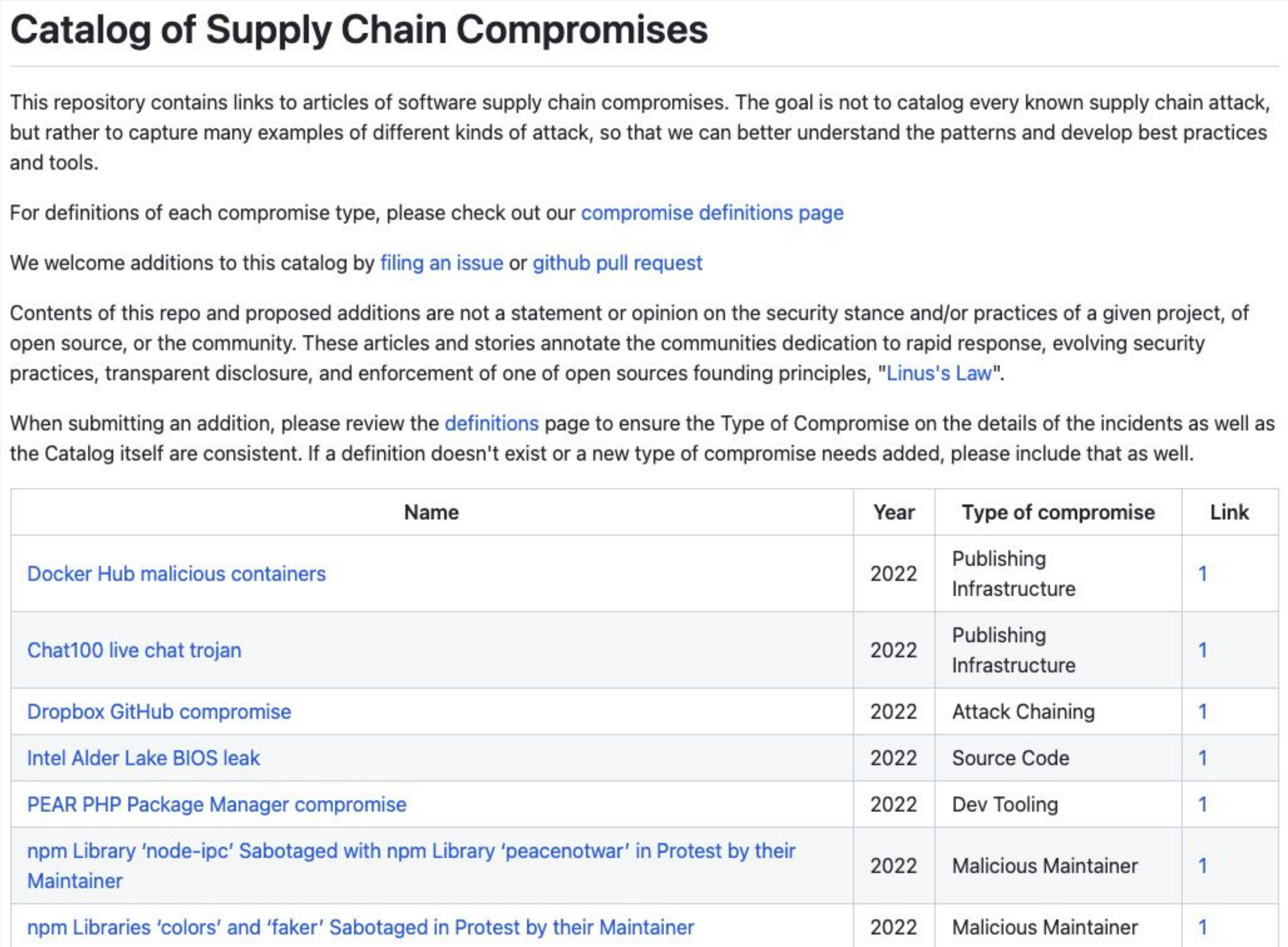
Verify source code

- Do you require signed commits?
- Do you use git hooks or automated scans to prevent committing secrets to source control?
- Have you defined an unacceptable risk level for vulnerabilities? For example: no code may be committed that includes Critical or High vulnerabilities
- Do you use automated scanning to detect and prevent security issues, vulnerable dependencies, etc. from being committed to the repo that are not in compliance with your defined risk threshold?
- Have you defined clear contributors roles? Are they documented and discoverable?
- Do you enforce review and approval of contributions prior to merging?
- Are branch protection rules in place?
- Do you enforce MFA and SSH keys for human-entities? Do you have a plan in place for rotating SSH keys at regular intervals or following a key leak?
- Do you limit the access of automation agents (like CI/CD pipelines) following the principles of least privilege and just-in-time?

Verify materials

- Do you verify that dependencies meet your minimum thresholds for quality and reliability?

Publications



Catalog of Supply Chain Compromises

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

Contents of this repo and proposed additions are not a statement or opinion on the security stance and/or practices of a given project, of open source, or the community. These articles and stories annotate the communities dedication to rapid response, evolving security practices, transparent disclosure, and enforcement of one of open sources founding principles, "Linus's Law".

When submitting an addition, please review the definitions page to ensure the Type of Compromise on the details of the incidents as well as the Catalog itself are consistent. If a definition doesn't exist or a new type of compromise needs added, please include that as well.

Name	Year	Type of compromise	Link
Docker Hub malicious containers	2022	Publishing Infrastructure	1
Chat100 live chat trojan	2022	Publishing Infrastructure	1
Dropbox GitHub compromise	2022	Attack Chaining	1
Intel Alder Lake BIOS leak	2022	Source Code	1
PEAR PHP Package Manager compromise	2022	Dev Tooling	1
npm Library 'node-ipc' Sabotaged with npm Library 'peacenotwar' in Protest by their Maintainer	2022	Malicious Maintainer	1
npm Libraries 'colors' and 'faker' Sabotaged in Protest by their Maintainer	2022	Malicious Maintainer	1

Doing research on real world supply chain compromises?
Come look at the list!

Know about a supply chain compromise?
Create a PR to add to the list!

In Progress – Get Involved!

Light weight threat modelling

tag-security-Issue #903

Cloud Native Security Whitepaper

3.0 tag-security issue #975
Audio CNS WP Audio Recording v2 · Issue #953

Cloud Native Security Controls Mapping

CNCF Supply Chain Security Tools Mappings · Issue #984

Cloud Native Security Controls Mapping to NIST· Issue #845

Security assessments

KubeVela · Issue #976

KubeEdge · Issue #974

cert-manager · Issue #949

Keptn · Issue #784

Flux multi-tenancy proposal · Issue #896

Zero Trust whitepaper

Zero Trust - Cloud Native Platforms and Services · Issue #950

Catalog of Supply Chain Compromises

https://github.com/cncf/tag-security/tree/main/supply-chain-security/compromises

TAG Security

Who we are

What we do

🦝 How is this creating cloud native security?

Where to jump in

Awareness through effort

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

- Collaboration with related groups
  - K8s sig-security (disambiguation!)
  - K8s policy working group
  - Cloud Security Alliance
  - OpenSSF (SLSA, supply chain)

- Presentations increase awareness of open source security challenges, solutions, and futures
  - Security focused project presentations
    - Kubescape - tag-security 962
    - OpenFGA - https://github.com/cncf/tag-security/issues/902
    - Kubewarden - https://github.com/cncf/tag-security/issues/899

      and many more

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

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

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

Get involved now!

KubeVela · Issue #976

KubeEdge · Issue #974

Flux multi-tenancy proposal · Issue #896

cert-manager · Issue #949

Keptn · Issue #784

TAG Security

Who we are

What we do

How is this creating cloud native security?

🦝 Where to jump in

Join us!

CNCF Workspace
#tag-security

tag-security issues

good first issue help wanted

@cncfsecurityTAG

Roadmap
TAG Security Roadmap

CNCF TAG Security mailing list

CNCF TAG Security Calendar

CNCF TAG Security - YouTube

In Progress – Get Involved!

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

Light weight threat modelling

tag-security-Issue #903

Cloud Native Security Controls Mapping

CNCF Supply Chain Security Tools Mappings · Issue #984

Cloud Native Security Controls Mapping to NIST· Issue #845

Zero Trust whitepaper

Zero Trust - Cloud Native Platforms and Services · Issue #950

Cloud Native Security Whitepaper

3.0 tag-security issue #975
Audio CNS WP Audio Recording v2 · Issue #953

Security assessments

KubeVela · Issue #976

KubeEdge · Issue #974

cert-manager · Issue #949

Keptn · Issue #784

Flux multi-tenancy proposal · Issue #896

Catalog of Supply Chain Compromises

https://github.com/cncf/tag-security/tree/main/supply-chain-security/compromises

Thank you!

CLOUDNATIVE

SECURITYCON

NORTH AMERICA 2023