Chainguard

Parochial Suggestions on Open Source Developer Tools for Security

Helping NIST Consider Tools for a Proof-of-Concept DevSecOps Project

John Speed Meyers
Monday, September 19, 2022

My Mission

Make suggestions about what mature open source tools NIST should consider for its proof-of-concept and explain why.

I have not performed an exhaustive analysis of all open source security tools related to DevSecOps. (Yikes!)

So what is this based on?

- R&D at IQT Labs on open source software security
- R&D at Chainguard, a software supply chain security company
- My experience as an open source software developer of no particular repute

Areas of Focus

secure
container base images

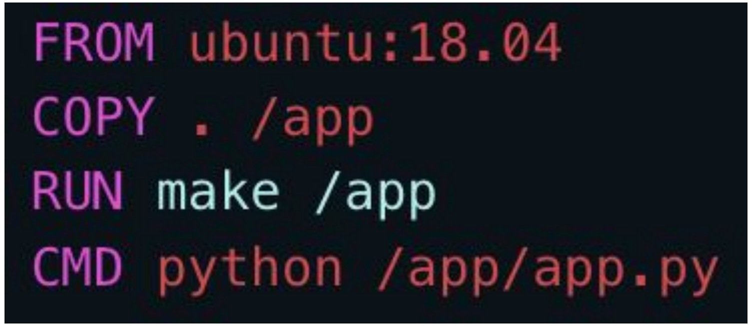
signing
software

static analysis during
continuous integration

secure container base images

secure container base images

The FROM command in a Dockerfile is the ultimate import statement

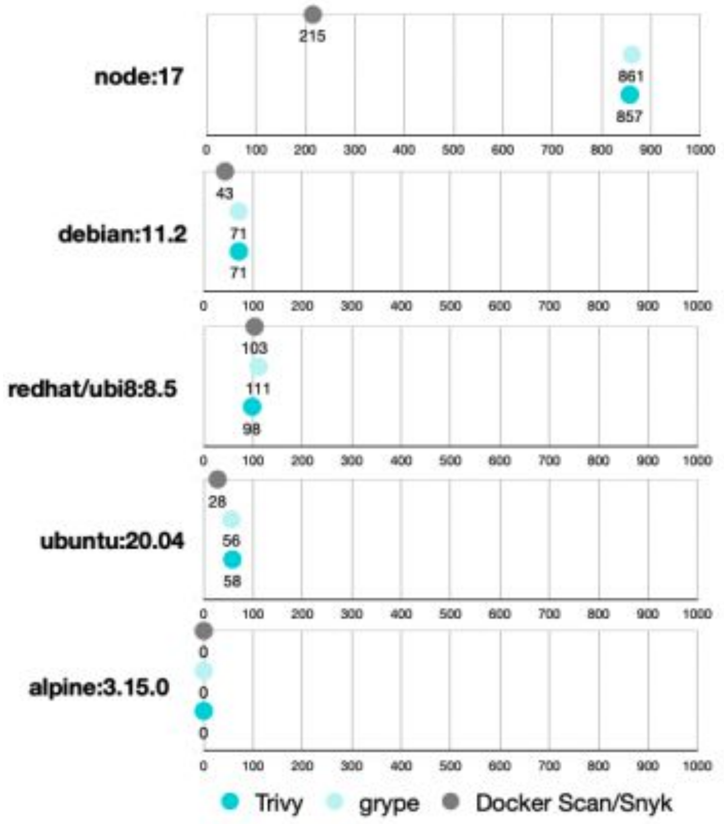


```
FROM ubuntu:18.04
COPY . /app
RUN make /app
CMD python /app/app.py
```

Source: Docker, “Best Practices for Writing Dockerfiles,” 2022, https://docs.docker.com/develop/develop-images/dockerfile_best-practices/

secure container base images

Popular open source base images can have tens or hundreds of known vulnerabilities



Source: Meyers and Newman, “All About That Base Image,” Chainguard Whitepaper, 2022.

secure container base images

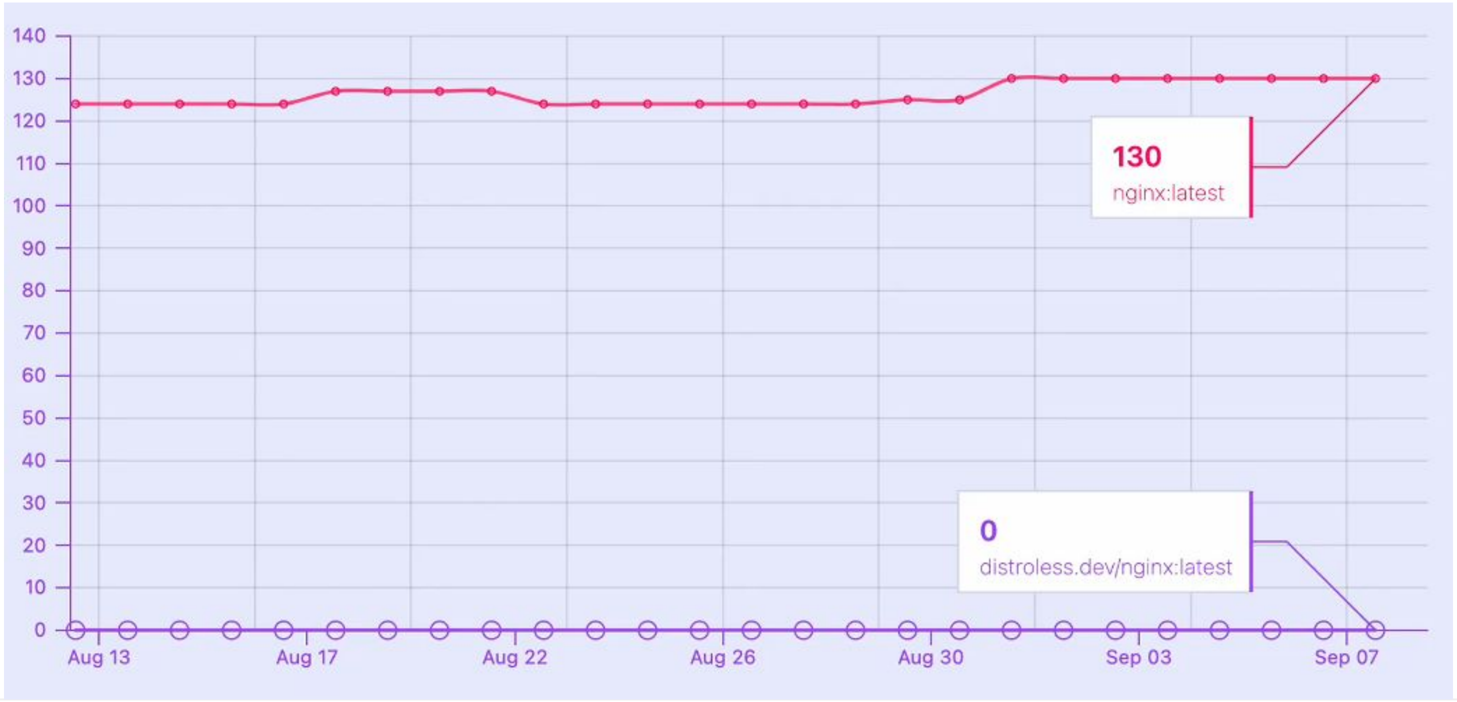
apko offers an alternative method of building minimal, secure-by-default base images

```
    _      ____    _  __   ___
   / \    |  _ \  | |/ /  / _ \
  / _ \   | |_) | | ' /  | | | |
 / ___ \  |  __/  | . \  | |_| |
/_/   \_\ |_|     |_|\_\  \___/
apko
```

https://github.com/chainguard-dev/apko

Apko-built images can have dramatically reduced CVE counts

# CVEs



Chainguard

Source: Daily trivy scan of nginx:latest and distroless.dev/nginx:latest

Sigstore: code signing is for everyone

Code signing is an empirically rare phenomenon

In most* programming language ecosystems, hardly anyone** signs software artifacts.

* Maven is an exception.

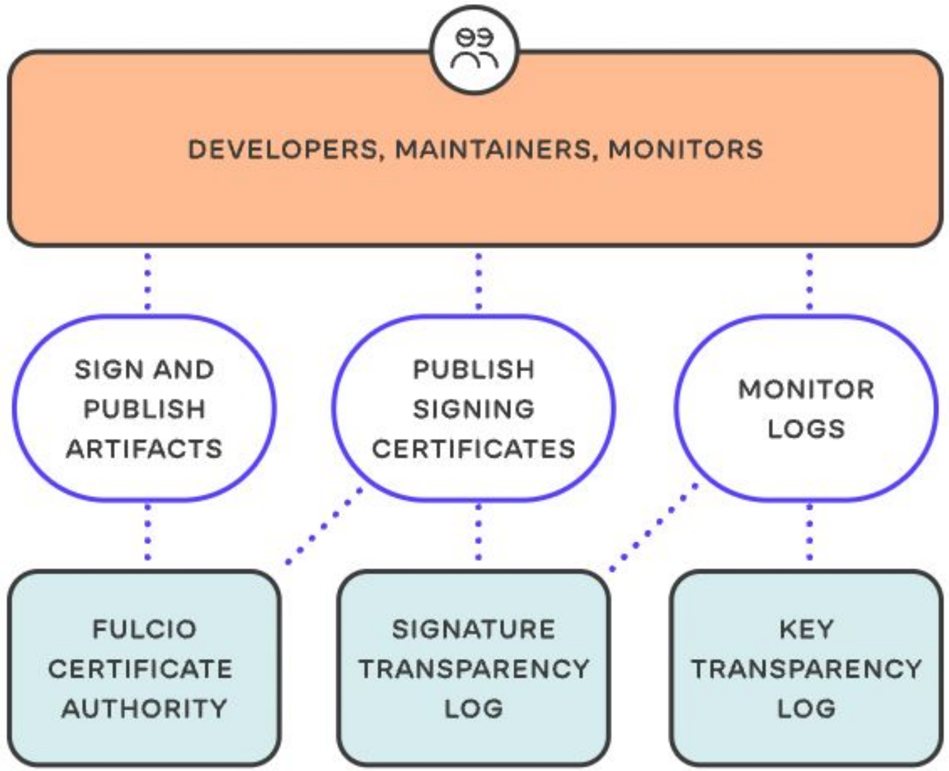
** < 5 percent

Why?

- PGP was designed for super-users
- Storing long-lived private keys is a pain
- Acquiring code signing certificates can be onerous and expensive
- among others…

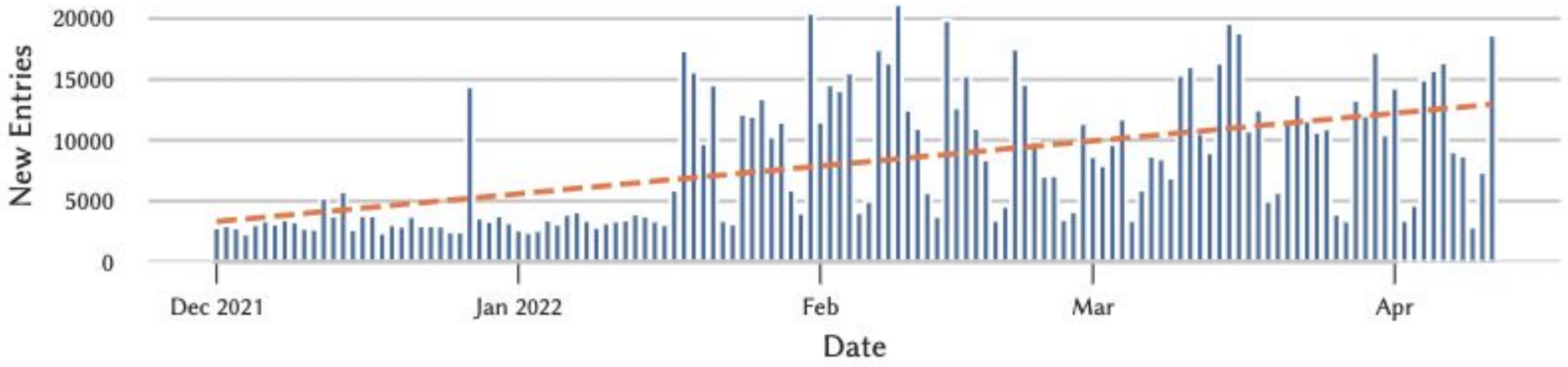
Source: Newman, Meyers, and Torres-Arias, "Sigstore: Signing is for Everyone," ACM CCS, 2022, forthcoming.

Sigstore simplifies signing


DEVELOPERS, MAINTAINERS, MONITORS
SIGN AND PUBLISH ARTIFACTS
PUBLISH SIGNING CERTIFICATES
MONITOR LOGS
FULCIO CERTIFICATE AUTHORITY
SIGNATURE TRANSPARENCY LOG
KEY TRANSPARENCY LOG

Source: sigstore.dev

Sigstore usage is growing!



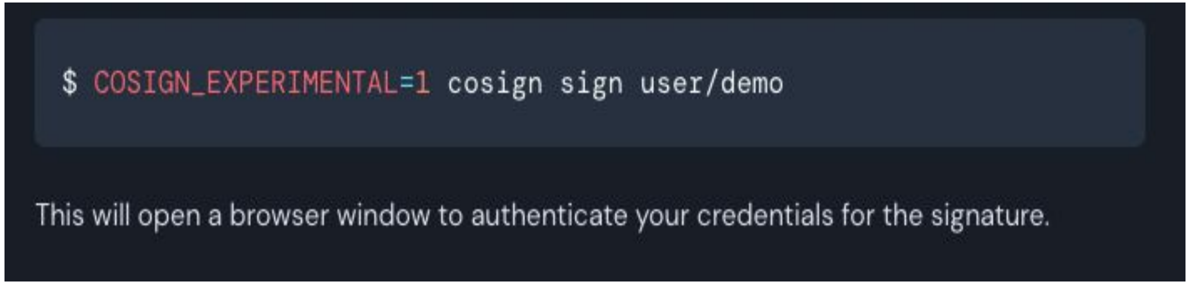
Chainguard

Source: Newman, Meyers, and Torres-Arias, “Sigstore: Signing is for Everyone,” ACM CCS, 2022, forthcoming.

from the user's perspective

Involves a command line tool or GitHub Action

https://github.com/sigstore/cosign



```
$ COSIGN_EXPERIMENTAL=1 cosign sign user/demo
```

This will open a browser window to authenticate your credentials for the signature.

Source: sigstore.dev

static analysis during continuous integration

scan all code going into your codebase

scan

static analysis is cheap and cheerful

all code

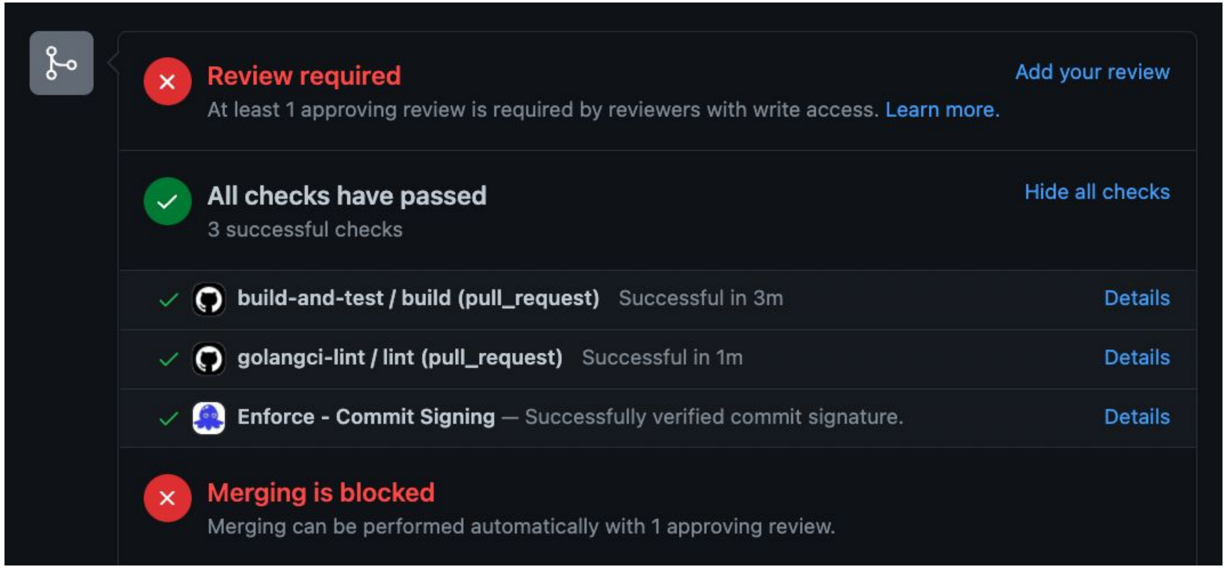
at least the code you write

but scanning dependencies too is nice

golangci-lint is a combination of linters for Go

https://github.com/golangci/golangci-lint

What it practically means: checks pass before a commit to main gets merged



Review required
At least 1 approving review is required by reviewers with write access. Learn more.
Add your review

All checks have passed
3 successful checks
Hide all checks

✓ build-and-test / build (pull_request) Successful in 3m Details
✓ golangci-lint / lint (pull_request) Successful in 1m Details
✓ Enforce - Commit Signing — Successfully verified commit signature. Details

Merging is blocked
Merging can be performed automatically with 1 approving review.

Chainguard

Parochial Suggestions on Open Source Developer Tools for Security

Helping NIST Consider Tools for a Proof-of-Concept DevSecOps Project

John Speed Meyers
Monday, September 19, 2022