Chainguard Libraries

The why, what, and how for building your applications with libraries you can trust

Manfred Moser

Manfred Moser

Victoria, BC, Canada
Sr. Principal DevRel Engineer at Chainguard
Open source hacker and advocate, author, teacher, presenter, and host

manfred.moser@chainguard.dev

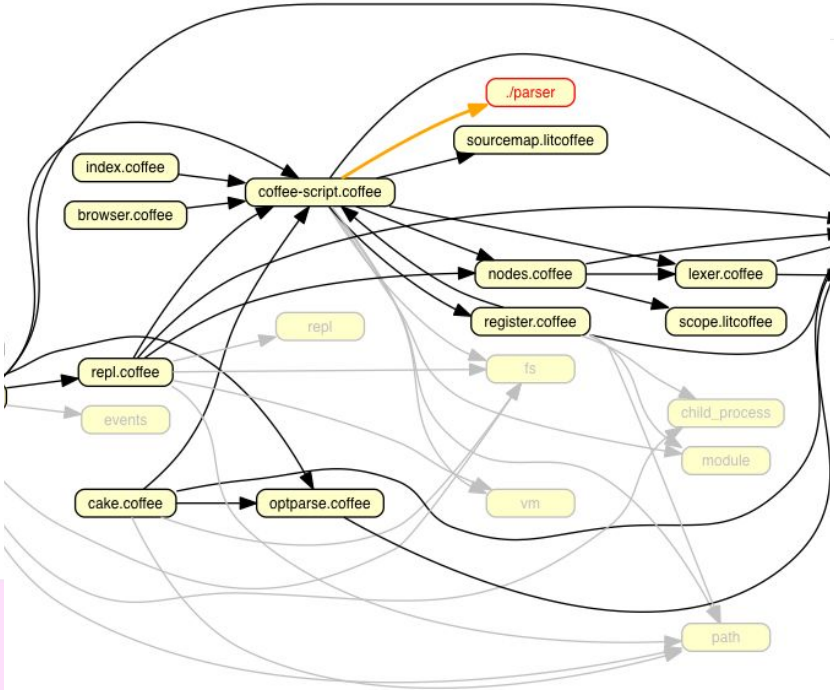
Agenda

- Why?
  - Software supply chain attacks
- What?
  - Chainguard Libraries - we build from source and serve
- How?
  - Hands on demos of Chainguard Libraries features
- Questions
  - Any time but also at end of session

Software supply chains

Should you be worried?

Software supply chains



- Software is built on other software
- Proprietary software is **impossible** without open source
- “Transitive Dependencies”

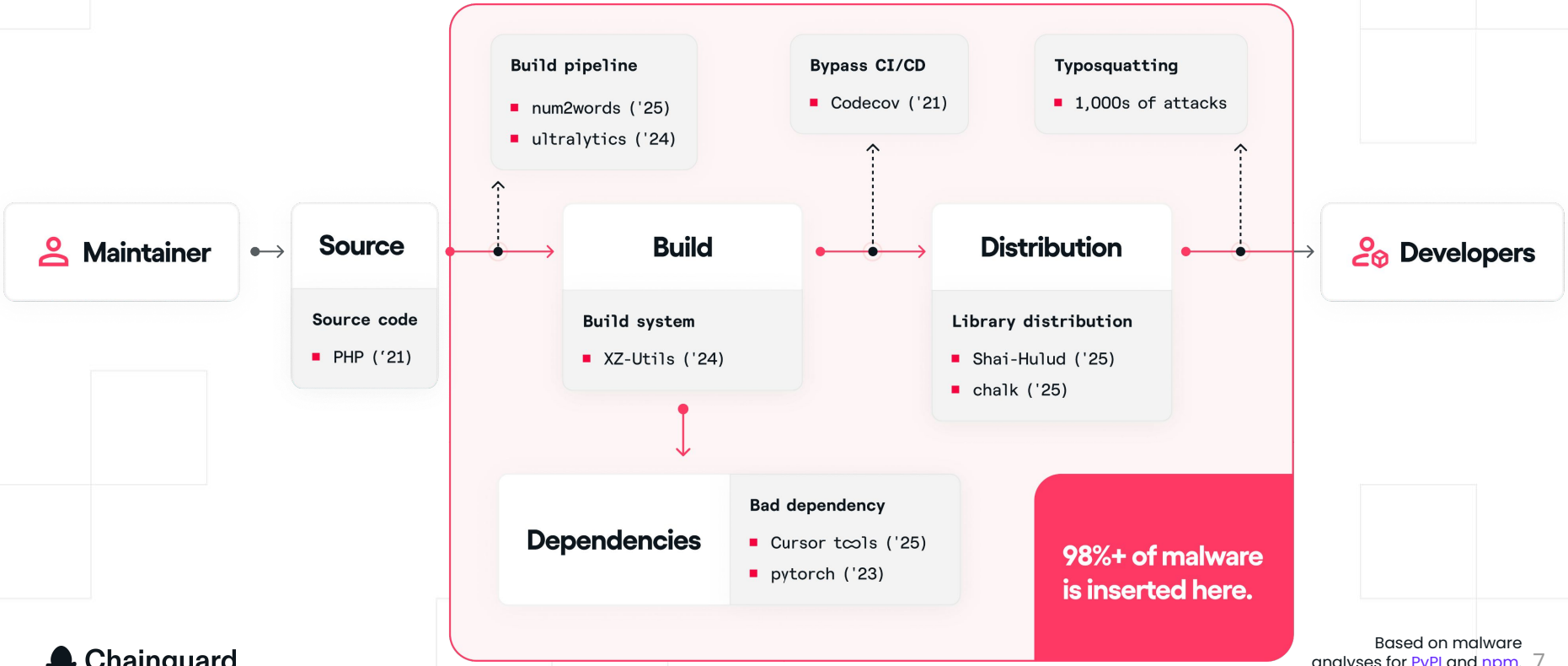
Software supply chain speedrun

Raw materials to
finished product

Complex, fast moving network

Many actors, many steps

Many potential points of failure



Chainguard

Based on malware analyses for PyPI and npm.

Long history of supply chain attacks

- 2020 - Solarwinds/Sunburst Russian attack
- 2021 - log4shell remote code execution
- 2022/2023 - PyTorch dependency confusion
- 2024 - Ultralytics YOLO
- 2025 - the year of the sand worms
- 2026 - Trivy and litellm

Shai Hulud - Malware rides the Worm

Sampling of other noteworthy attacks and methods

Future threats and trends – the struggle continues

All public indexes are scrambling

- Playing catch-up
- Underfunded
- Understaffed
- Huge workload for operators
- Trusted Publishing

Juicy targets lead to sophisticated attacks

2026: The year of AI-assisted attacks

Attacks intensify

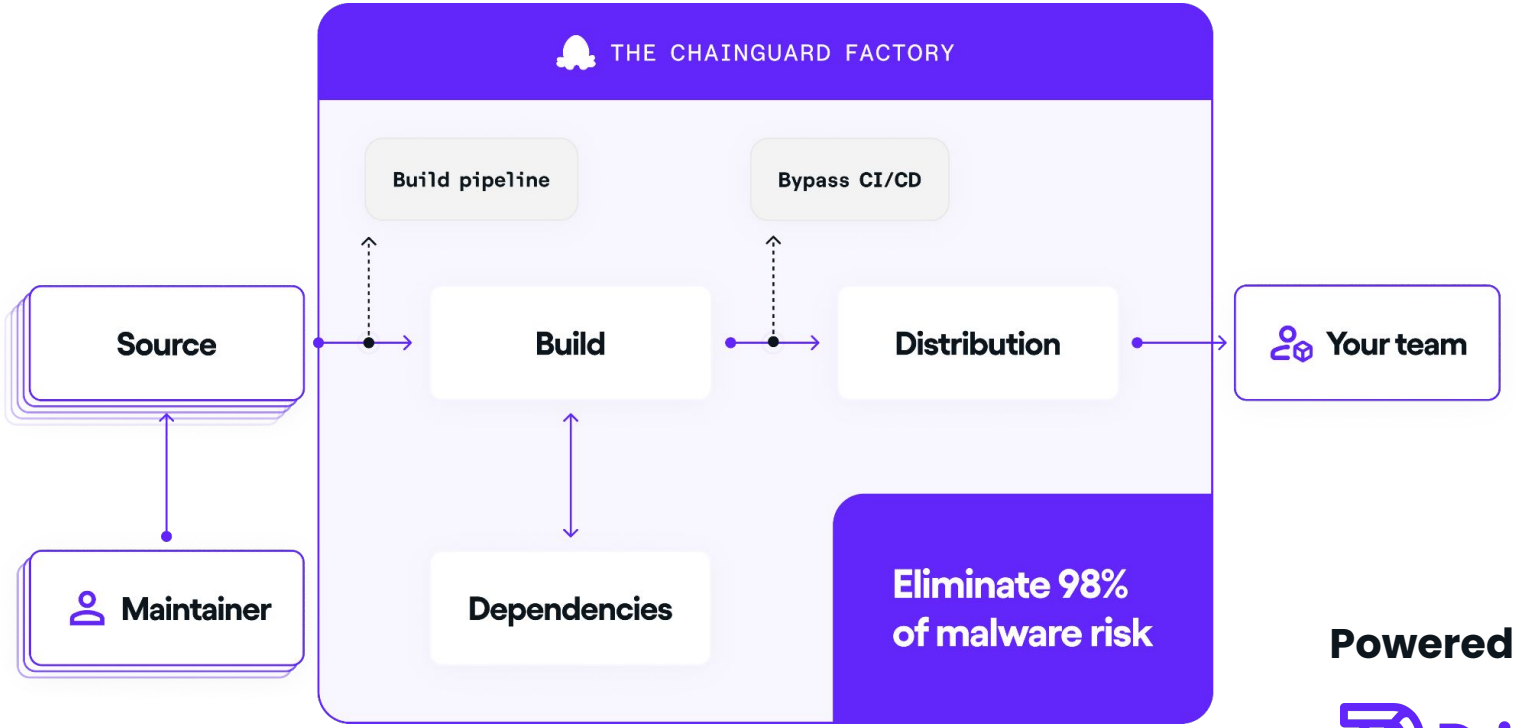
- 560,000 new malware samples daily
- 108 new vulns daily
- 44 days to exploit
- $16.6 billion cybercrime losses in 2024

Incidents

Chainguard Libraries

An overview leading to demos and deep dives

Chainguard Agentic Factory as your supplier



Powered by DriftlessAF

Chainguard

Chainguard Libraries

- Built from **source** - no source, no binary
- Secure, trusted replacement for public repos
- No malware
- No ghost releases
- SBOM details
- Provenance info

Thousands of libraries, with more added every day

Python

Replaces libs from PyPI

Support for pip, uv, poetry

Django	flask	numpy	requests
matplotlib	scikit-learn	CUDA	
fast	pandas	... and 16K+ more!	

Remediating critical and high-severity CVEs

Thousands of libraries, with more added every day

Python

Replaces libs from PyPI

Support for pip, uv, poetry

Django	flask	numpy	requests
matplotlib	scikit-learn	CUDA	
fast	pandas	... and 16K+ more!	

Remediating critical and high-severity CVEs

Java

Replaces libs from Maven Central

Support for Apache Maven, Apache Ant, Gradle, Bazel

Google Guava	Apache Commons	akka	
scala	springboot	jackson	lombok
log4j	kotlin	... and 57K+ more!	

Thousands of libraries, with more added every day

Python

Replaces libs from PyPI

Support for pip, uv, poetry

flask | numpy | requests

fast | otlib | scikit-learn | CUDA

pandas | ... and 16K+ more!

Remediating critical and high-severity CVEs

Java

Replaces libs from Maven Central

Support for Apache Maven, Apache Ant, Gradle, Bazel

Google Guava | Apache Commons | akka

scala | springboot | jackson | lombok

log4j | kotlin | ... and 57K+ more!

JavaScript

Replaces libs from npm Registry

Support for npm, pnpm, yarn berry, yarn classic

react | debug | lodash | chalk | colors

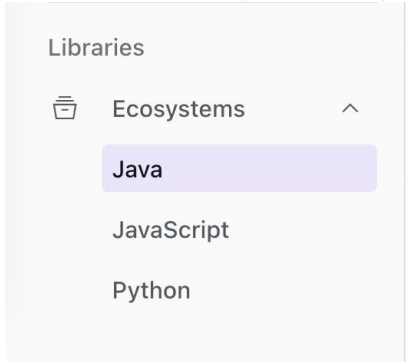
express | async | moment | prop-types

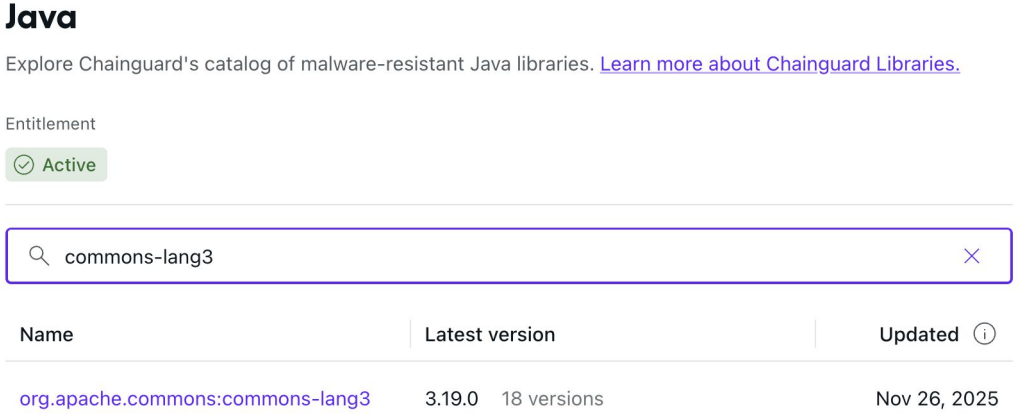
request | axios | ... and 18K+ more!

Excludes pre- and post-install scripts by design as they've been known to carry malware

Chainguard console

- Select ecosystem and inspect count
- Browse, search, and filter
- View versions
- Inspect remediation info for backport
- Pull tokens





Chainguard Libraries access

- chainctl command line tool for pull token
- Alternatively use console
- Use env variables or store as secrets
- Use in web browser for browsing

```
 ~ $ chainctl auth pull-token --output env --repository=java

   ✔ Selected organization chainguard.edu.
Creating new java library pull-token in chainguard.edu

export CHAINGUARD_JAVA_IDENTITY_ID=45a0c61ea6fd977f050c5fb9ac06a6
export CHAINGUARD_JAVA_TOKEN=eyJhbGciOiJSUzI1NiJ9.eyJhdWQiOiJodHR
6MTc3NzA1ODY0MiwiaWF0IjoxNzc0NDY2NjQyLCJpc3MiOiJodHRwczovL3B1bGx0
dWIiOiJwdWxsLXRva2VuLWMyZTYzNzU0ZDAyZWY2MzRmNTg5NGJlNDk3ZjMwYTA4M
YXtlHunhpFbkAroA9YYfyHhn7NvwlXMW_Leq2-5b3EbHZ1C3eiKeA4Q4q944FIhHB
K_Yo4sWVMQUHtm4WCKhlU_-Z7lOV6n9pJK_n1zzxmEYNyoy3MDdL7n4-oWopDzhtV
```

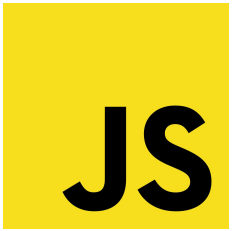
More browsing

Use pull token and URL in web browser:

- Simple index for Python
  - https://libraries.cgr.dev/python/
  - Wheels and sdist files
  - Packaged, native dependencies
  - Variants around gcc, Python, and distro
- Maven repository browsing
  - https://libraries.cgr.dev/java/
  - All files - including SBOM and provenance

Direct access demos

For initial testing without a repository manager
It’s demo time.



But what if a library is not found?

Chainguard Repository

Libraries

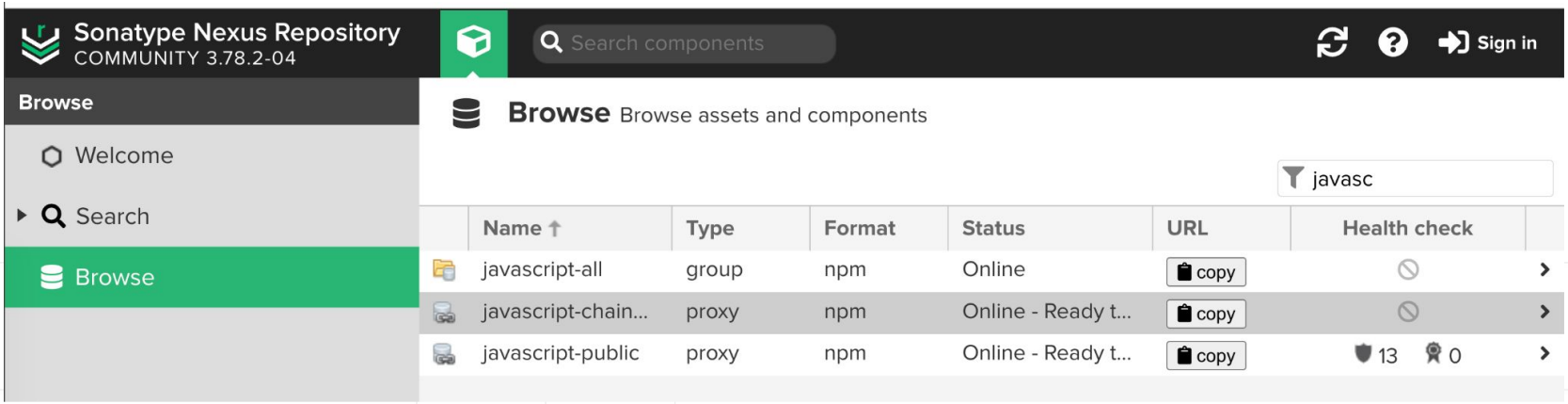
Chainguard Repository

- Available for JavaScript
- Fallback to npm Registry for unavailable packages
- Adds a **global** cooldown period, tool independent
- Blocks malware

Single, trusted access point for all needed packages

Repository managers

- For enterprise use
- Manage your private packages
- Seamless access to Chainguard Libraries



Verification

```
$ chainctl libraries verify
flask-3.0.1-py3-none-any.whl

Artifact: flask-3.0.1-py3-none-any.whl

Verification Coverage: 100%
```

- Use chainctl
- Checks signatures and provenance info
- Works on dev projects, binaries, and containers

Q&A

There are no bad questions,

so go on and ask.

APRIL 2 @ 1:30PM ET

Malware unpacked: The Trivy attack, how it happened, and what to do now

Dan Lorenc, CEO & Founder, Chainguard
Reid Tatoris, VP of Product, Chainguard

APRIL 9 @ 1PM ET

What's new: Product announcements, feature releases, and roadmap

Explore our latest product announcements and how we're using AI to deliver a secure-by-default experience.

APRIL 23 @ 1PM ET

Learning lab: Securing CI/CD with Chainguard

Erika Heidi, Staff DevRel Engineer, Chainguard

Thank you

Manfred Moser