chainguard

Learning Lab:

Chainguard Libraries

JavaScript
Python CVE remediation

Meet your trainer

- Open source hacker and advocate
- Book author, teacher, presenter, and host
- Trino, Maven, Nexus, and more
- Dad, builder, biker, boarder, yogi, gardener, ...
- Victoria, BC, Canada

- manfred.moser@chainguard.dev

Manfred Moser

Agenda

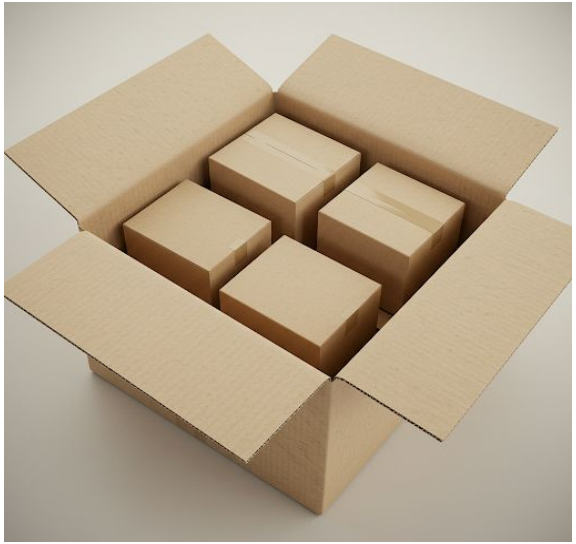
- Introduction
- Fundamental concepts around Chainguard Libraries
- Specifics for Chainguard Libraries for JavaScript
- CVE remediation for libraries
- Demo with Chainguard Libraries for Python
- Q&A

Secure containers are great ....

But what's inside?

Applications

Containers run your applications



… with lots of libraries inside.

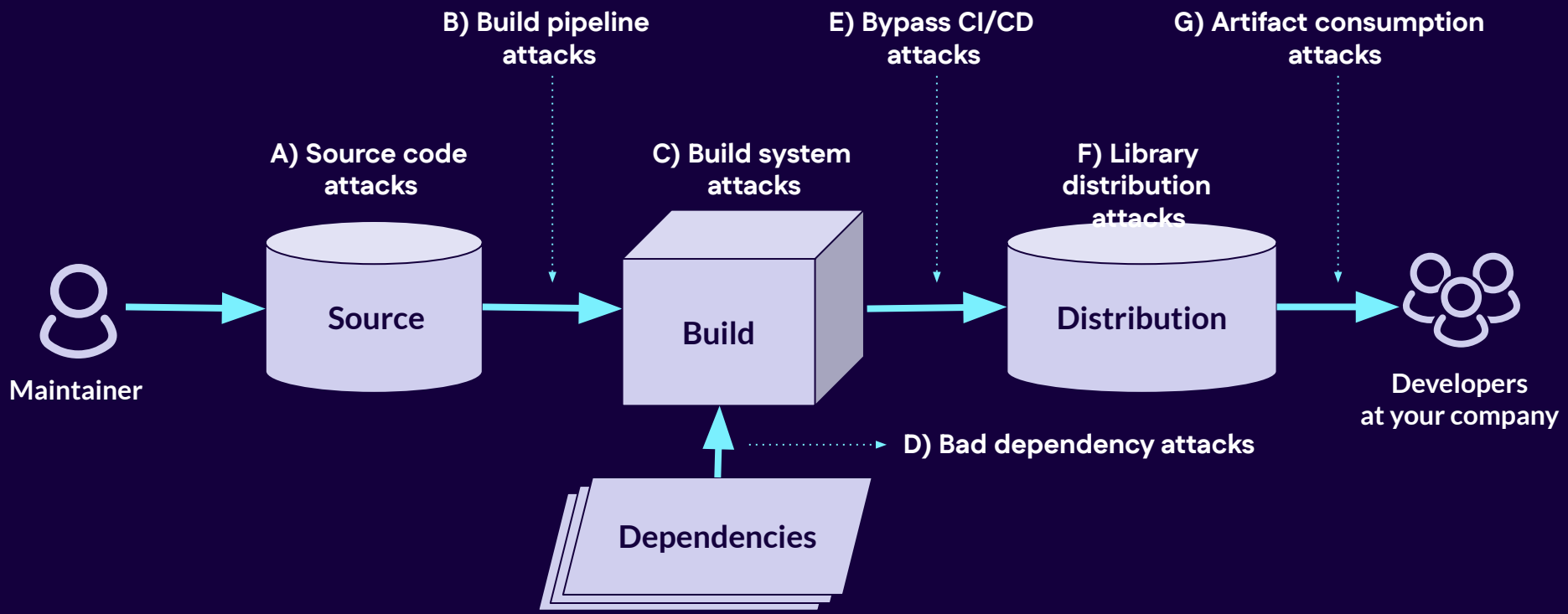
Outside containers

Even outside containers - your application is built from (open source) components.

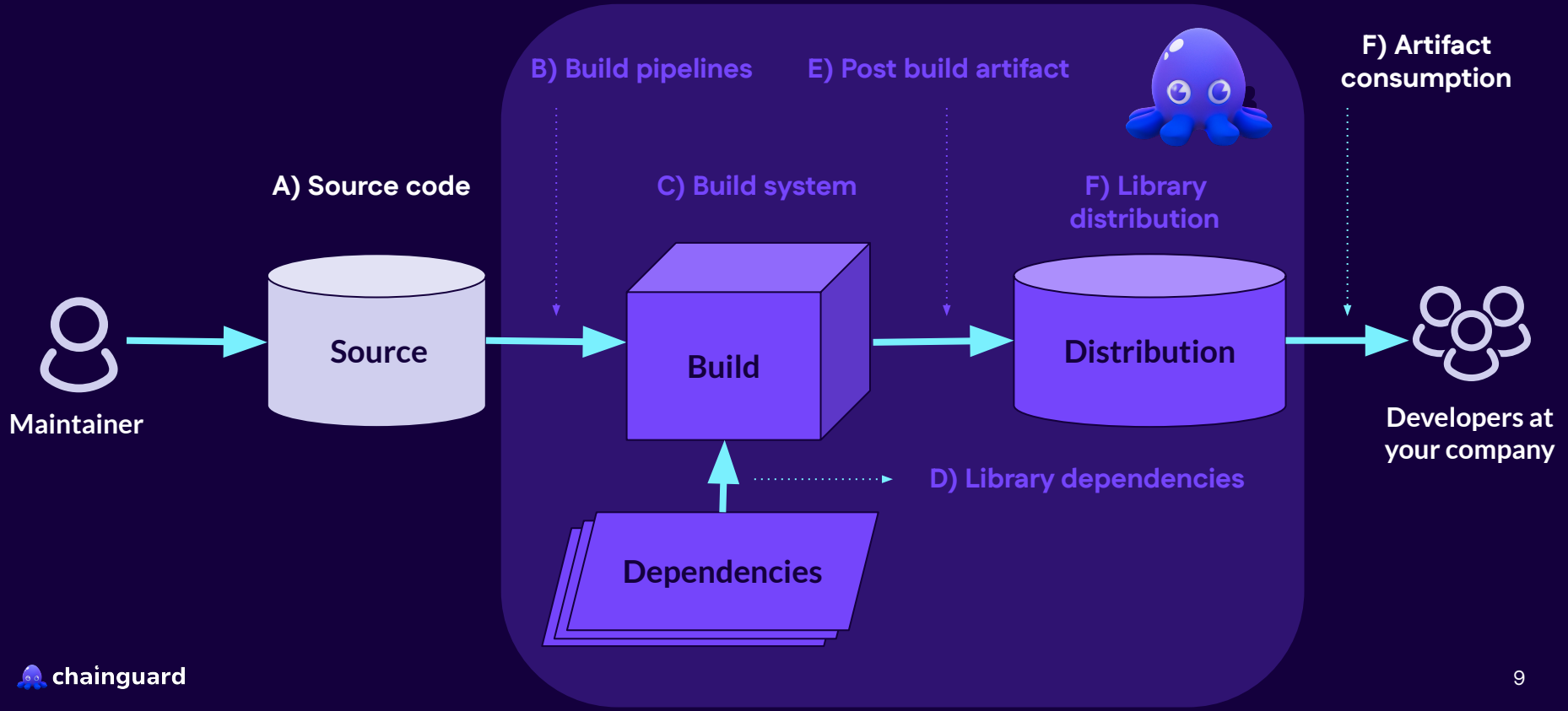
So what is a library?

- Building blocks for your application
- Specific feature set and capabilities
- Well beyond 70% of your application
- Typically open source
- Different names across language ecosystems
- In all shapes and sizes

Package lifecycle and types of supply chain attacks



Chainguard Libraries eliminate supply chain attacks at build and distribution



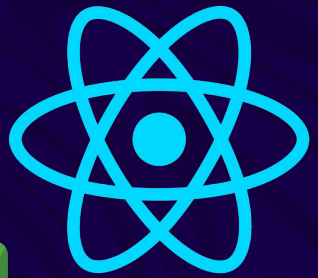
Chainguard Libraries

Bringing the successful approach from containers to application developer.

Build from source!

chainguard

Chainguard Libraries for



JavaScript ecosystem

- Very large and diverse ecosystem
- JavaScript and TypeScript languages
- Multiple runtime environments
  - Web browsers Chrome, Firefox, Safari
  - Server runtimes Node.js, Deno, Bun

    https://en.wikipedia.org/wiki/List_of_server-side_JavaScript_implementations
- Multiple JS engines - V8, SpiderMonkey, JavaScriptCore

  https://en.wikipedia.org/wiki/List_of_JavaScript_engines

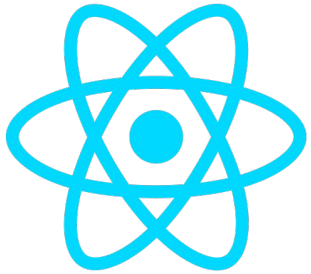
JavaScript packages

- npm packages
- Default and common package source **npm Registry** - https://www.npmjs.org/
- Over two million packages, constantly growing
- Common build and packaging tools are `npm`, `pnpm`, `yarn`, bun

Examples for JavaScript packages

You might recognize some of these names

- Front-end frameworks
  - React.js, Angular, Vue.js, Svelte, EmberJS
- Back-end frameworks
  - Node.js, Express, Nest.js
- Other frameworks
  - Nextjs, Nuxt, Gatsby
- Mixed libraries
  - lodash, D3.js, jQuery





No source - no package malware

npm malicious package analysis results:

- About 95 percent of the known malicious packages have no source
- Roughly 5 percent of the known malicious packages have no **matching** source

Chainguard Libraries for JavaScript **prevents >99 percent** of all malware attacks from npm Registry packages.

https://www.chainguard.dev/unchained/mitigating-malware-in-the-npm-ecosystem-with-chainguard-libraries

Chainguard Libraries for JavaScript

- Packages from npm Registry
- Built from source in Chainguard Factory
- New registry as replacement at https://libraries.cgr.dev/javascript/
- No malware
- No insecure pre/post install scripts

Easy to use

Authenticate and use with a repository manager or directly:


```
pnpm config set registry https://libraries.cgr.dev/javascript/

npm config set registry
https://repo.example.com:8443/repository/chainguard-javascript/

yarn config set npmRegistryServer
https://repo.example.com:8443/repository/chainguard-javascript/
```

Clean cache and rebuild to refresh lock files.

Repository managers

- Preferred use with a private repository manager
- Direct access for testing

And others like Verdaccio, Google Artifact Registry, Cloudsmith, …

Other benefits from Chainguard Libraries

- Signed packages
- Full SLSA 2 attestation
- SBOM files
- Prevention of pre/post install script attacks
- Verification tool `chainver`

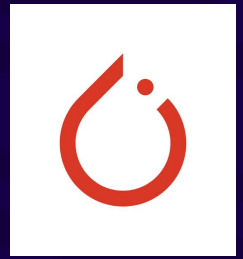
chainguard

Demo time

Chainguard Libraries for JavaScript

chainguard

Chainguard Libraries for



Chainguard Libraries for Python overview

- Generally available
- Includes CVE remediation for popular packages
- Supports build and packaging tools `pip`, uv, `poetry`
- Growing security scanner support `grype`, `trivy`

What is CVE remediation?

- Use available fixes from upstream project
- Backport to older releases as requested
- Enable users to get CVE remediation with minimal update
- Alternative to use newer version remains, but is often too much work

Details

- New patch release with each fix `1.2.3+cgr.1`
- Optional from separate repository

  https://libraries.cgr.dev/python-remediated/
- VEX feed for scanners

  https://libraries.cgr.dev/openvex/v1/all.json

CVE remediation example

- VEX feed data for Flask

  https://libraries.cgr.dev/openvex/v1/pypi/flask.openvex.json
- CVE-2023-30861, GHSA-m2qf-hxjv-5gpq
- GitHub security advisory contains
  - Links to PRs (pallets/flask@`70f906c`, pallets/flask@`afd63b1`)
  - Release 2.3.2 with fix
- Changes are backported to create versions in

  https://libraries.cgr.dev/python-remediated/simple/flask
- Tarball and wheel files - example flask-**2.0.2+cgr.1**
- Upgrade for user of 2.0.2 is **less risky and effort than updating to 2.3.2**

chainguard

Demo time

CVE remediation with Chainguard Libraries for Python

Further resources

- https://www.chainguard.dev/libraries
- https://edu.chainguard.dev/chainguard/libraries/
- https://edu.chainguard.dev/chainguard/libraries/javascript/
- https://edu.chainguard.dev/chainguard/libraries/python/
- https://edu.chainguard.dev/chainguard/libraries/cve-remediation/
- https://edu.chainguard.dev/chainguard/libraries/scanners/

Next up

- 13 November: **What's new from Chainguard - Product announcements and feature releases**
  - Presented by a panel of product managers and experts
  - https://go.chainguard.dev/whats-new-webinar
- 20 November: **Learning lab - Chainguard OS on Raspberry Pi**
  - Presented and demoed by Erika Heidi
  - https://go.chainguard.dev/learninglab-raspberrypi
- 10 December: **Beyond the Guardrails - The Next Wave of Secure Software Innovation**
  - Panel discussion of the Chainguard founders
  - https://go.chainguard.dev/FoundersPanelDec2025
  -

Questions

?

Thank you!

chainguard