Chainguard | Chains - KTH

The safe source for opensource

Peter Andersson

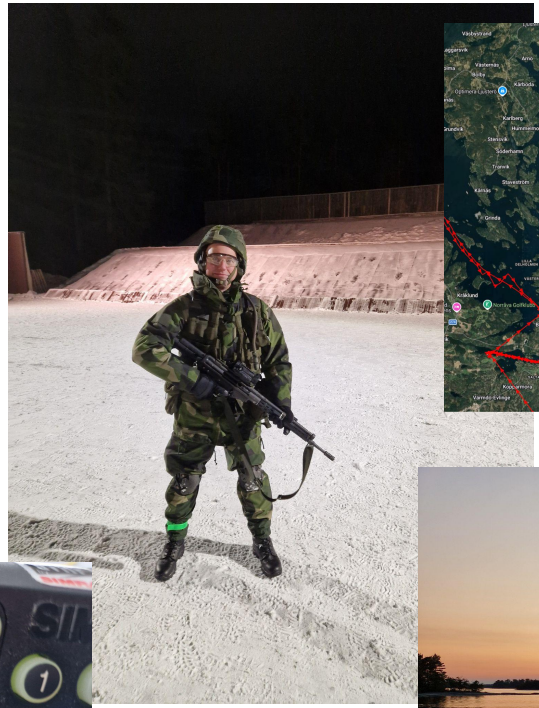
peter.andersson@chainguard.dev

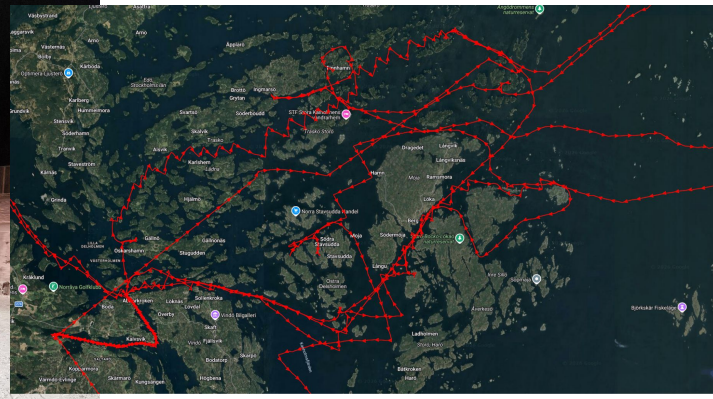
- Enterprise Sales Engineer
- M.Sc.E.E e94 Lunds Tekniska Högskola
- Open Source evangelist,
  “Free as free speech, not free beer”

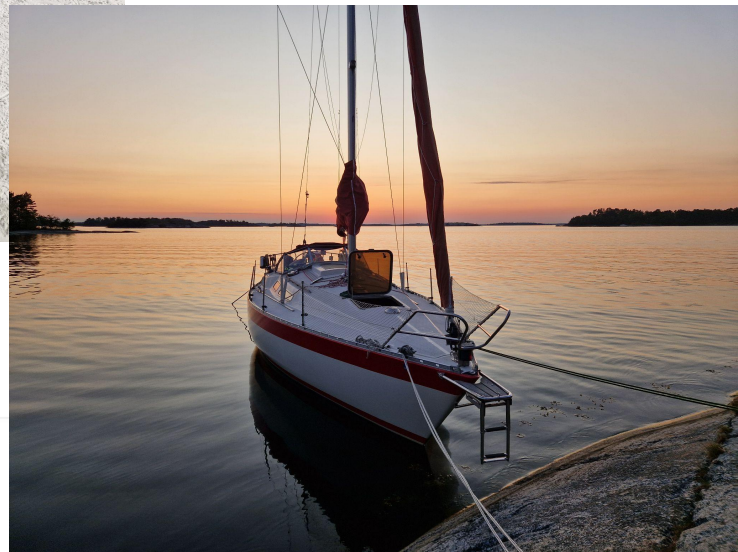
- Partner Sales Engineer, Broadcom
- Enterprise Sales Engineer, Sysdig
- Technical Strategist, Suse
- Senior Sales Engineer, Black Duck
- Product Manager, op5
- …

Spare time

- Just joined the Home Guard
- Sailing boat
- Train
- Fiddle with OSS,
  favourite project Signal-K







Chainguard

Typical CI/CD pipeline

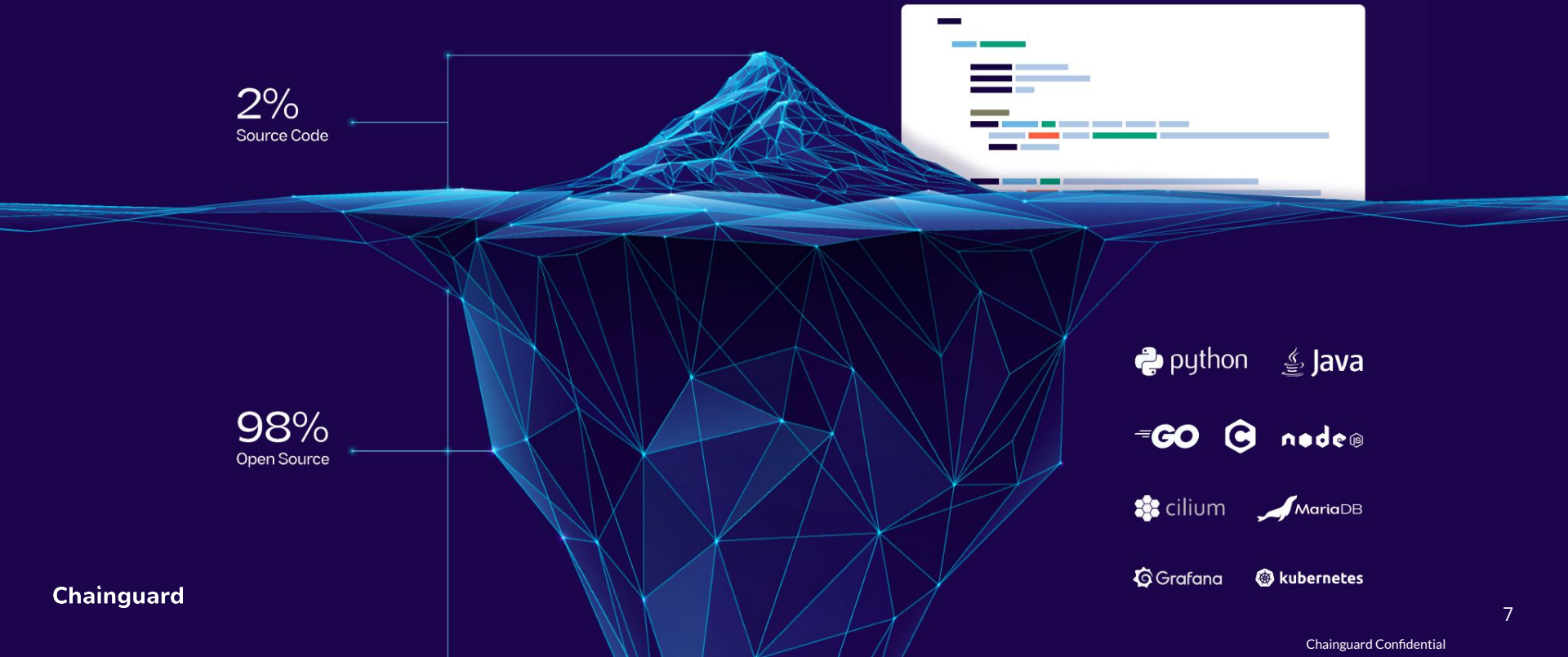
Typical CI/CD pipeline

Chainguard Secure

Typical CI/CD pipeline

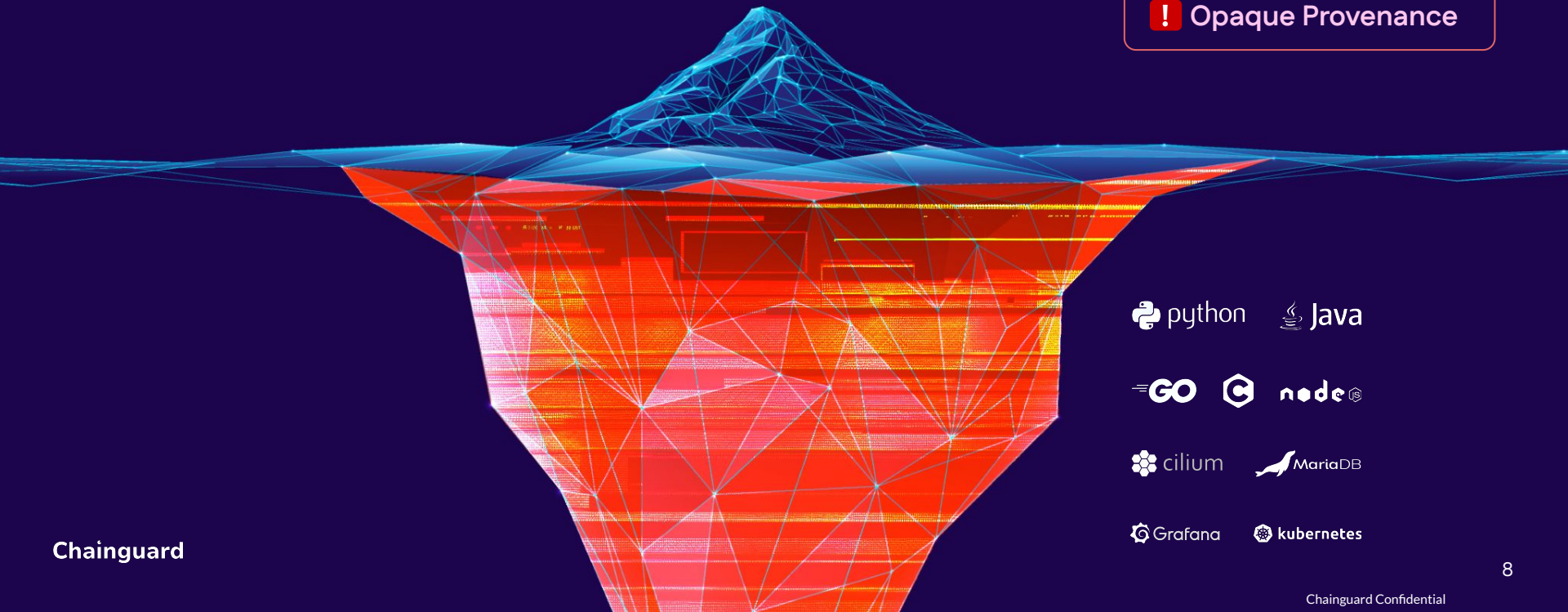
Chainguard Impact

Open Source Software Has Transformed Software Development



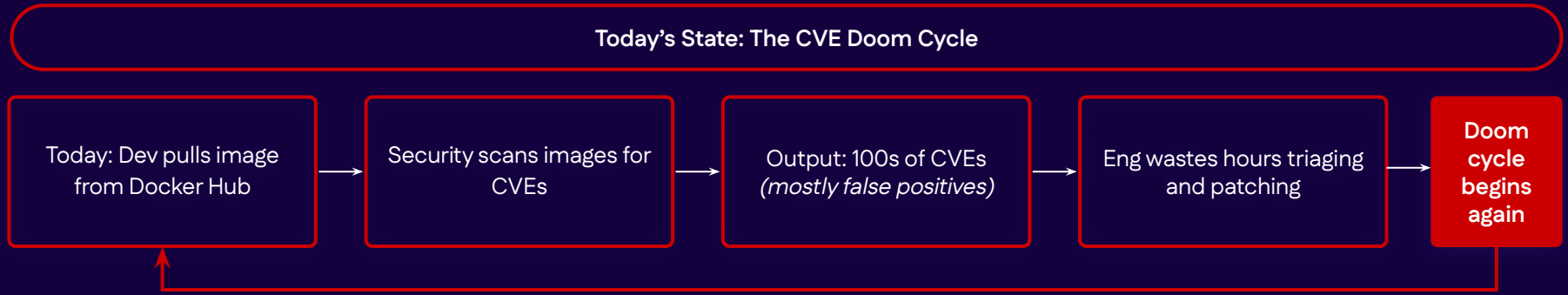
Traditional Open Source is an Insecure Foundation for Software Development

- ! Persistent CVEs
- ! Large Attack Surface
- ! Opaque Provenance



python Java GO C node.js cilium MariaDB Grafana kubernetes

The Status Quo for CVE Management is Deeply Broken



The old way of building with open source isn't working

CVEs Accumulate Quickly

Patches in dependencies can take months to reach a distro update.

Free Images Fall Short

To standardize secure-by-default, you have to build and harden yourself.

Bloated Artifacts & Patching Limitations

Unnecessary attack surface. Can't patch what you can't control, waiting for a project or distro.

Malware Attacks Quickly Spread

More severe attacks on npm and PyPI (e.g. Shai Hulud). Over 500k malicious packages in a year*.

Constant CVE Triage and Patching

Start over on patching with every version upgrade + alert fatigue + testing.

Costly Golden Image Programs

Not enough engineers, automation and focus to scale. Half of your images are not "top 20", with 98% of CVEs**

Broad Zero-day & CVE Exposure

CVEs that are out of reach. Large zero-day blast radius. Undiscovered zero-days don't have a patch.

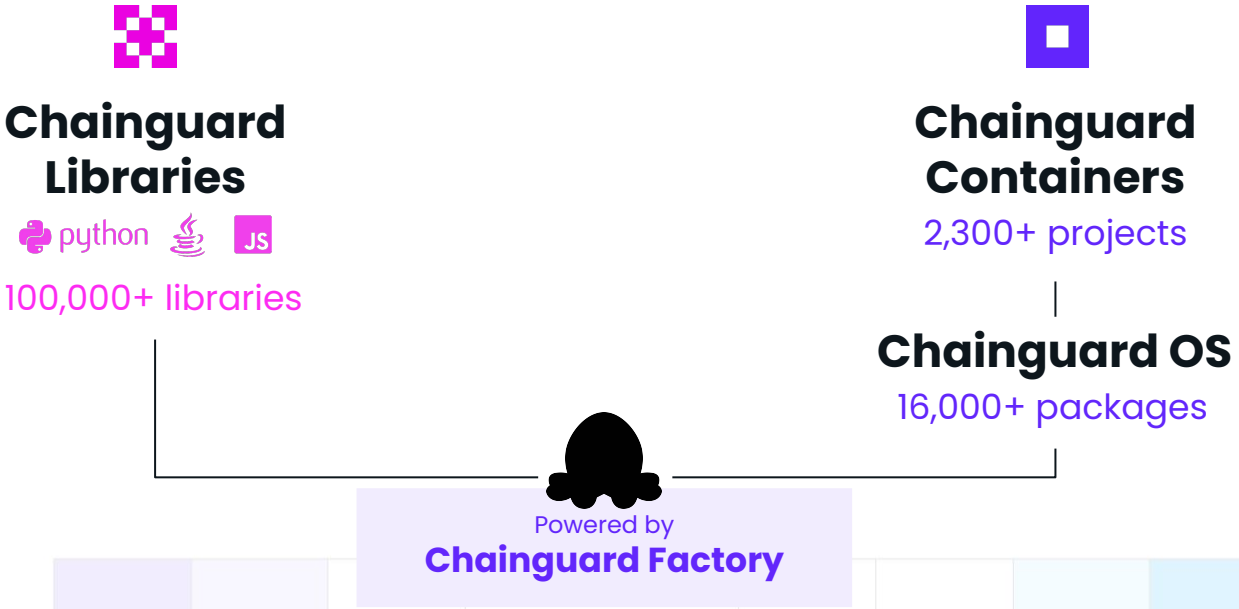
Scrambling to React to Attacks

If you're responding to malware, the damage is done. All you can do is chase the blast radius.

* Sonatype 2024 State of the Software Supply Chain®
** Chainguard The State of Trusted Open Source: December 2025

Chainguard: trusted open source for your entire stack

Customizable, reliable, compatible. Prevent attacks, eliminate CVEs and regain dev productivity.



Chainguard Containers: Minimal, zero-CVE images

Base Images

Build and run custom apps

python Java GO node

Custom Code

Toolchain / Runtime

System

Application Images

Run 3rd party apps

cilium MariaDB Grafana kubernetes

3rd Party Apps

Language Libraries

Runtime

System

- 2,000+ Projects, 300,000+ Image Artifacts
- Extensible and Customizable
- Helm Charts
- Signed SBOMs and Attestations
- FIPS-Validation and OS-Level STIGS

CVE Remediation SLA

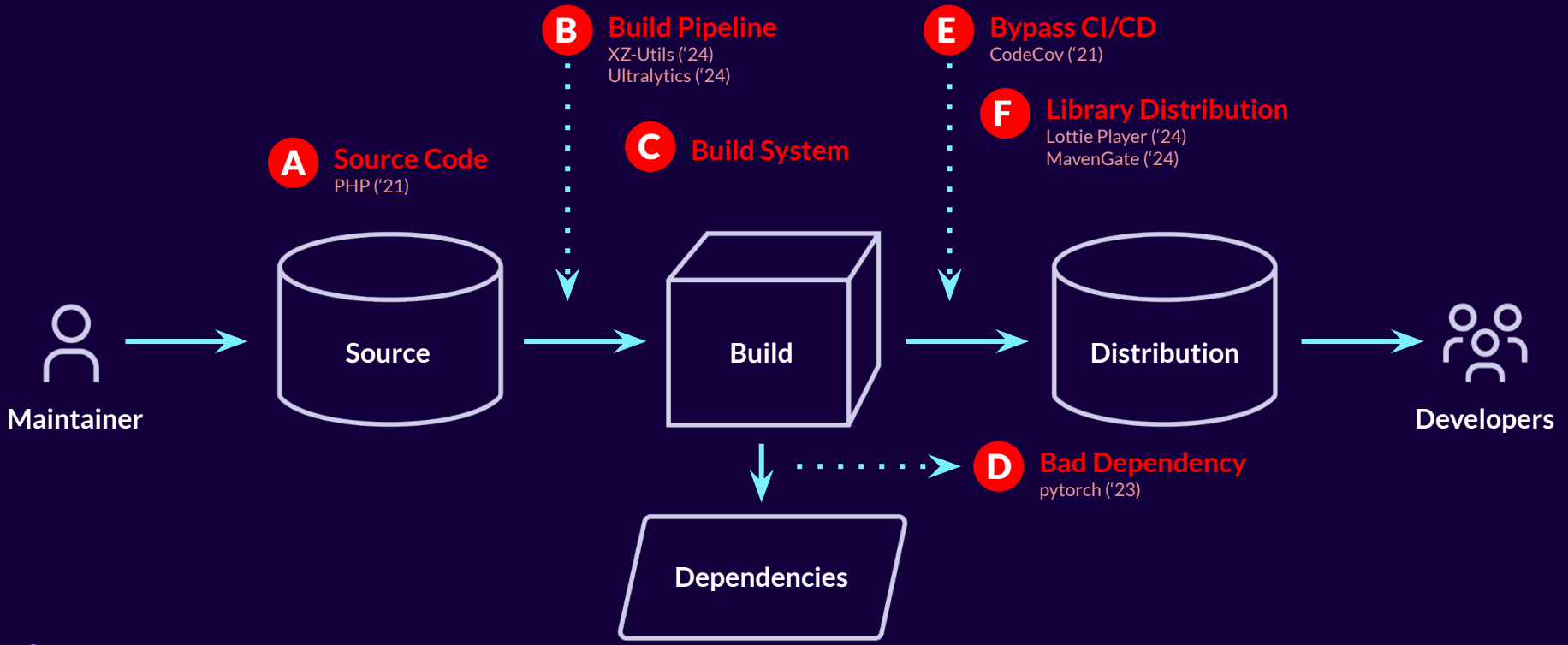
7 days for Critical

14 days for High / Med / Low

DEMO

- Go App on upstream Container
- Minimize the image and CVEs

The **frequency and severity of malware attacks** on the open source supply chain is growing rapidly



Introducing Chainguard Libraries

A trusted, malware-resistant source of libraries – built from source, with fewer CVEs.

Malware Mitigation

Prevent the growing risk of malware attacks from pulling libraries directly from public registries.

CVE Remediation

Avoid the security risk and engineering toil from remediating CVEs across open source libraries.

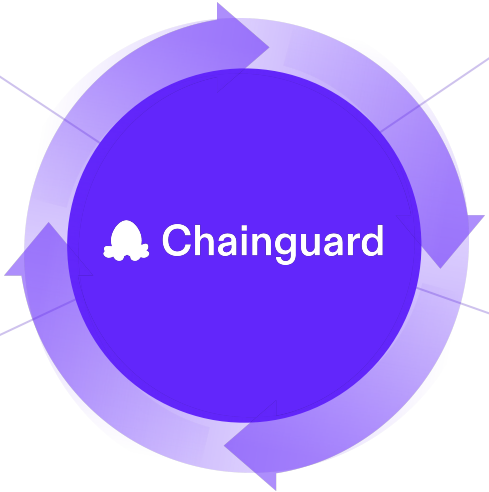
Powered by Chainguard Factory

Daily Builds from Source

- Every image built from the ground up
- Every package compiled from source code
- Complete control and provenance

Rigorous testing

- Unit, security, and acceptance tests
- OSS project test harnesses and novel approaches
- Ensure compatibility



Dependency Control

- Bump versions anywhere in the dependency tree (OS, toolchain, libraries, application)
- Optimize for minimal dependencies
- Backport patches for select Python libraries

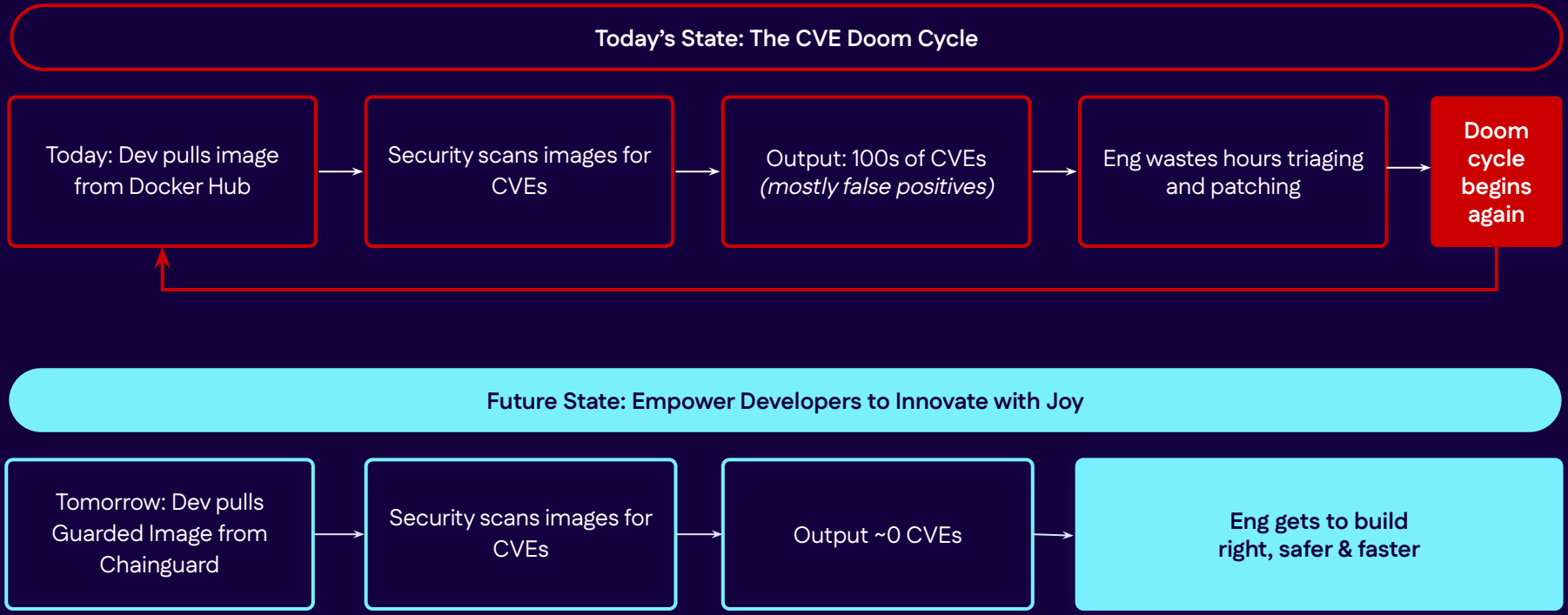
Cutting-edge Automation

- Automated and AI-based source code change detection, CVE triage, dependency bumps
- Automated rebuilds of 100,000+ packages and images for 1,800+ projects

DEMO 2

- Libraries

With Chainguard, ~~Shift Left~~ Start Left to Build Right



Thank you!

chainguard.dev

Test it out:
5 Free Images!