

Chainguard Libraries for Java



CVE remediation and upstream fallback

Manfred Moser, Sr Principal DevRel Engineer

Manfred Moser

Victoria, BC, Canada

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

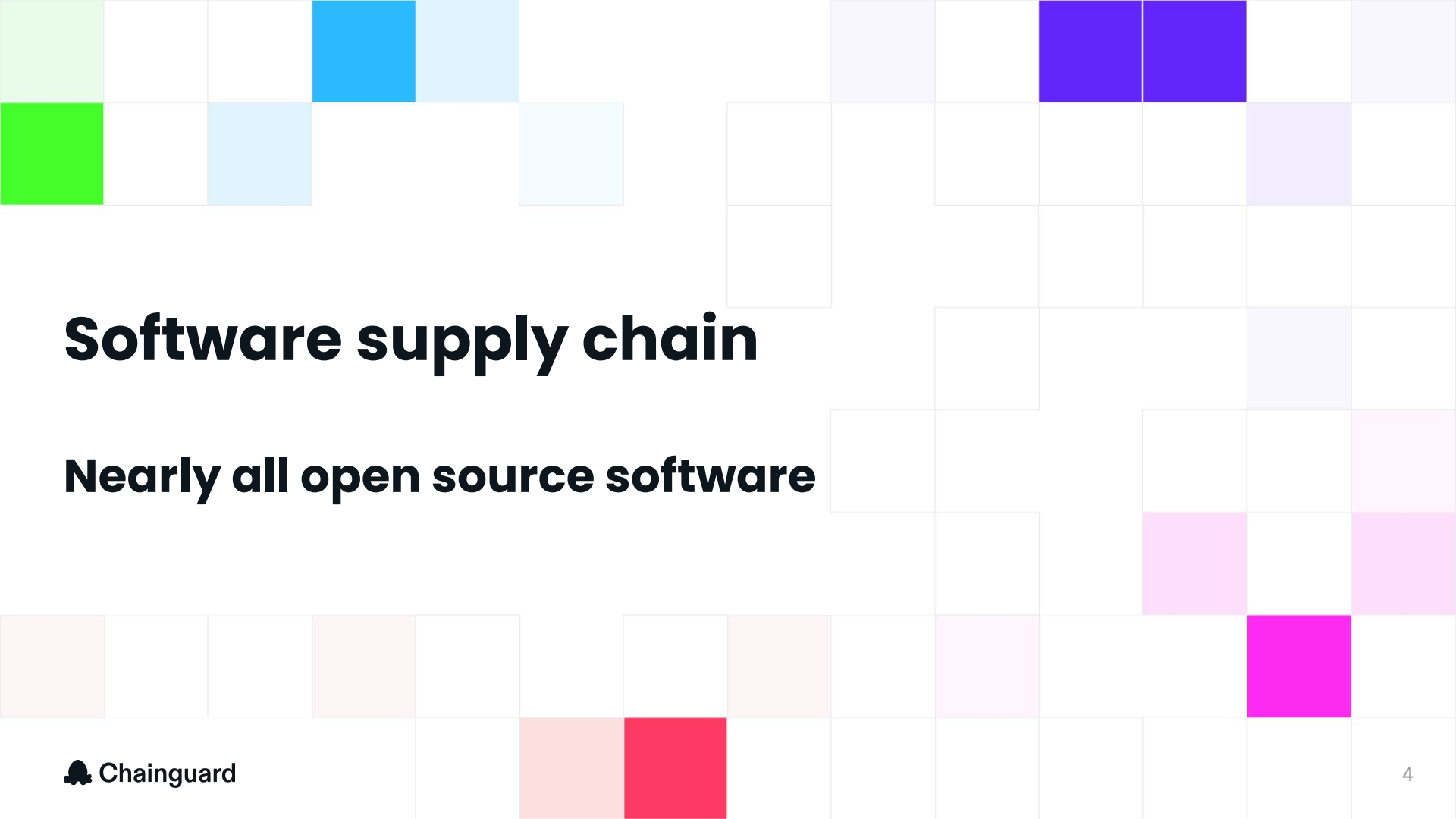
`manfred.moser@chainguard.dev`



Agenda

- Software supply chain security
- Chainguard Libraries overview
- CVE remediation
- Fallback and policies
- Demo
- Q&A

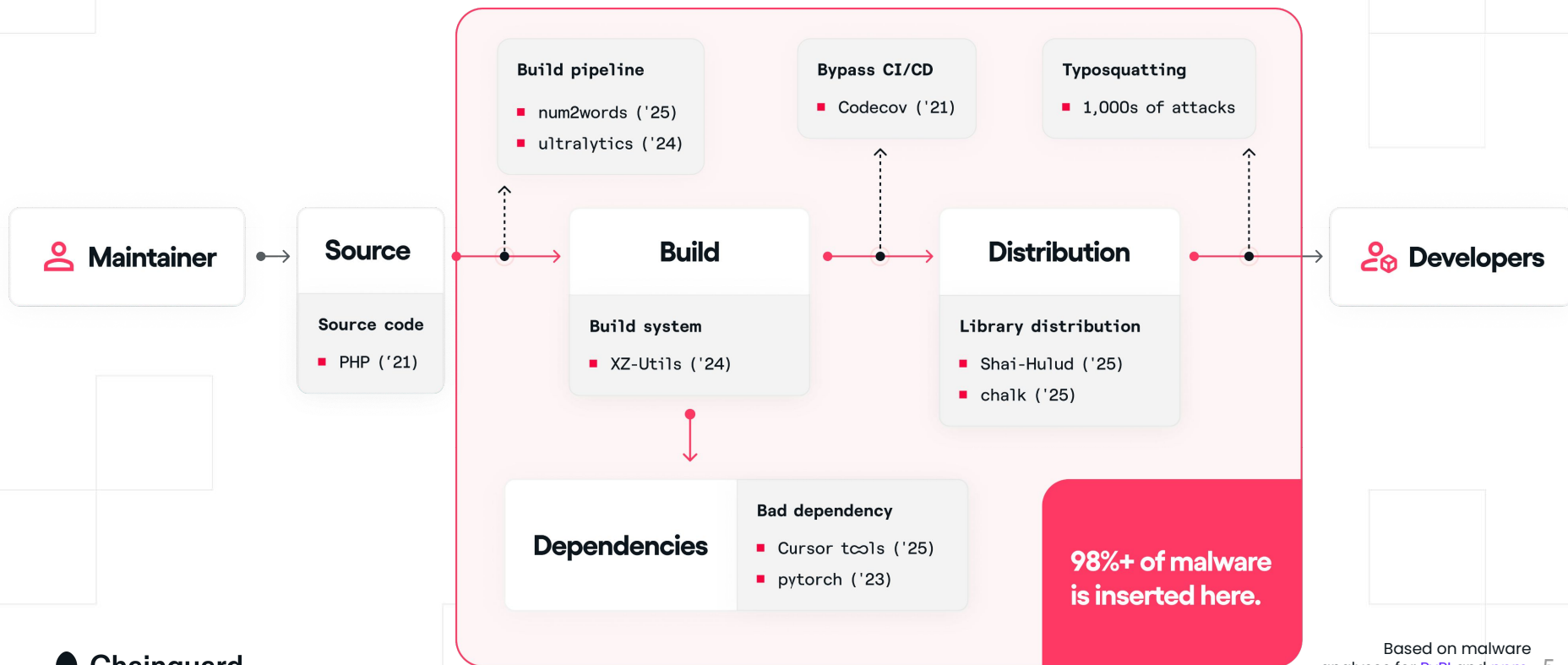




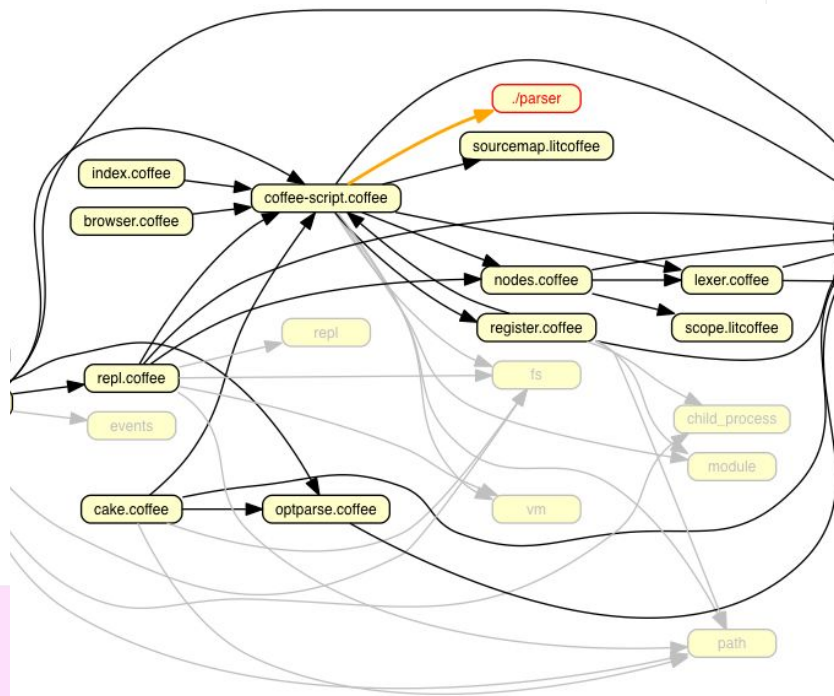
Software supply chain

Nearly all open source software

Many potential points of failure



Software supply chains



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

Long history of supply chain attacks

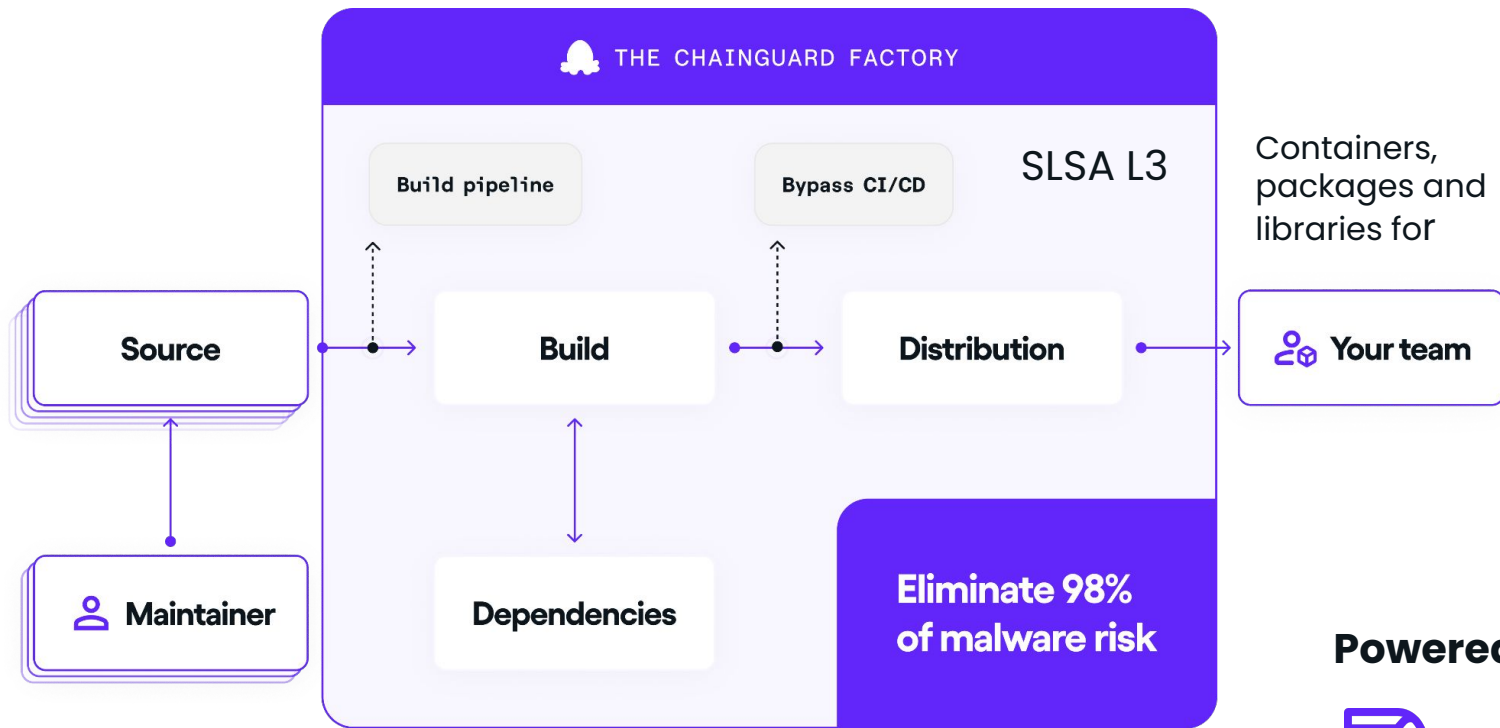


- 2020 – Solarwinds/Sunburst Russian attack
- 2021 – log4shell remote code execution
- 2022/2023 – PyTorch dependency confusion
- 2024 – Ultralytics YOLO
- 2025 – Shai Hulud – the year of the worms
- 2026 – Trivy, litellm, ...



Chainguard Libraries overview

Chainguard Agentic Factory as your supplier



Chainguard Libraries

- Built from **source**
 - no source, no Chainguard binary
- SBOM details and provenance info
- No malware, no ghost releases
- Secure, trusted replacement for public repos
- CVE remediation
- Fallback, cooldown, and policies

Chainguard Libraries



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 81K+ more!

Remediating critical and
high-severity CVEs

JavaScript

Replaces libs from npm

Support for npm, pnpm, yarn
berry, yarn classic

react debug lodash chalk colors

express async moment prop-types

request axios ... and 18K+ more!

CVE remediation

New for Chainguard Libraries for Java

REDUCE KNOWN RISK

Stay secure while you plan your next upgrade

- Java and Python CVE remediation
- Backporting upstream fixes for critical and high CVEs
- Run full testing suite, both baseline and regression
- Integrates with Gype, Trivy, AWS Inspector, and Anchore Enterprise

Flask

✓ REMEDIATED CVEs

LAST UPDATED 2 HOURS AGO

VERSION

[3.1.2+CGR.2](#)

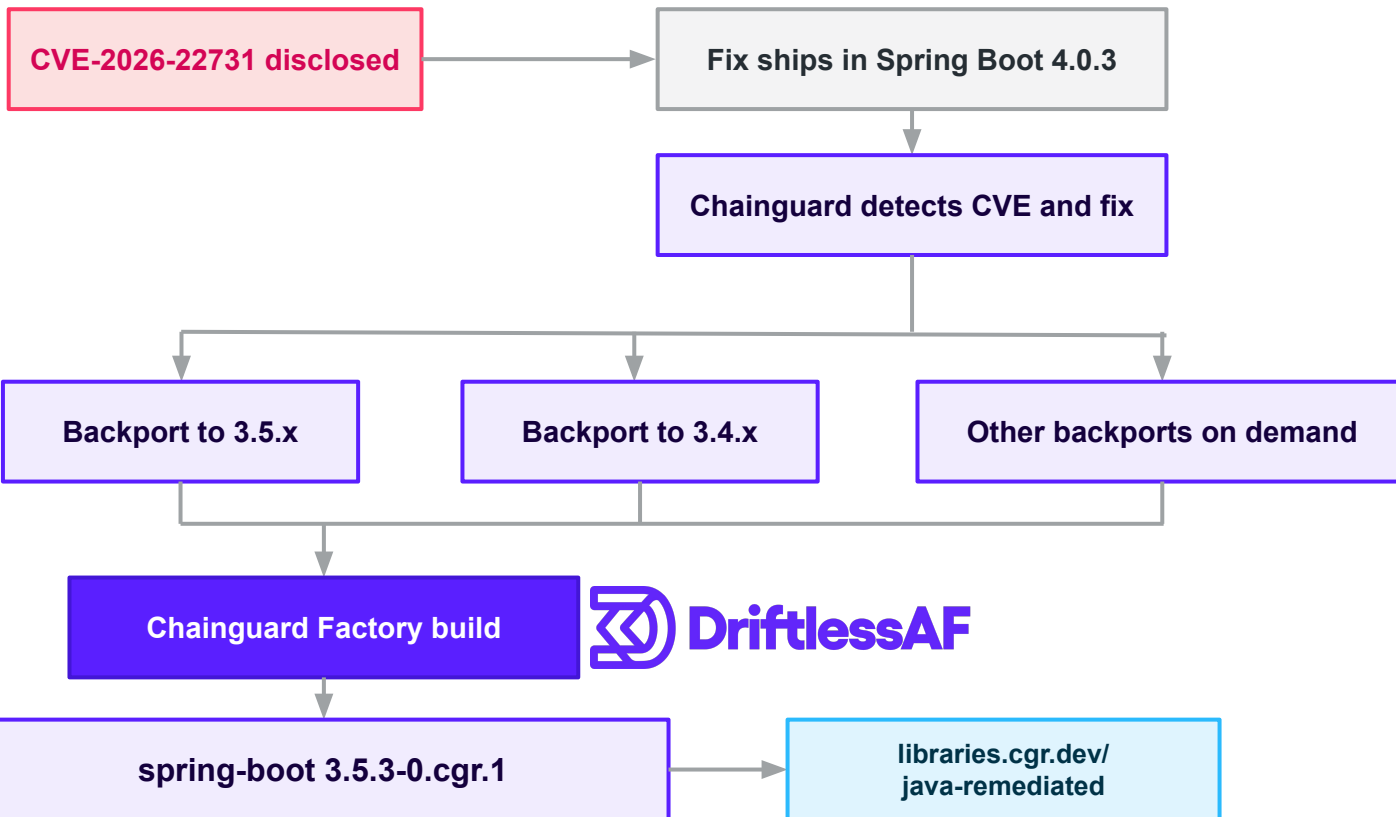
LATEST

✓ 3 RESOLVED CVEs

[3.1.2+CGR.1](#)

✓ 1 RESOLVED CVE

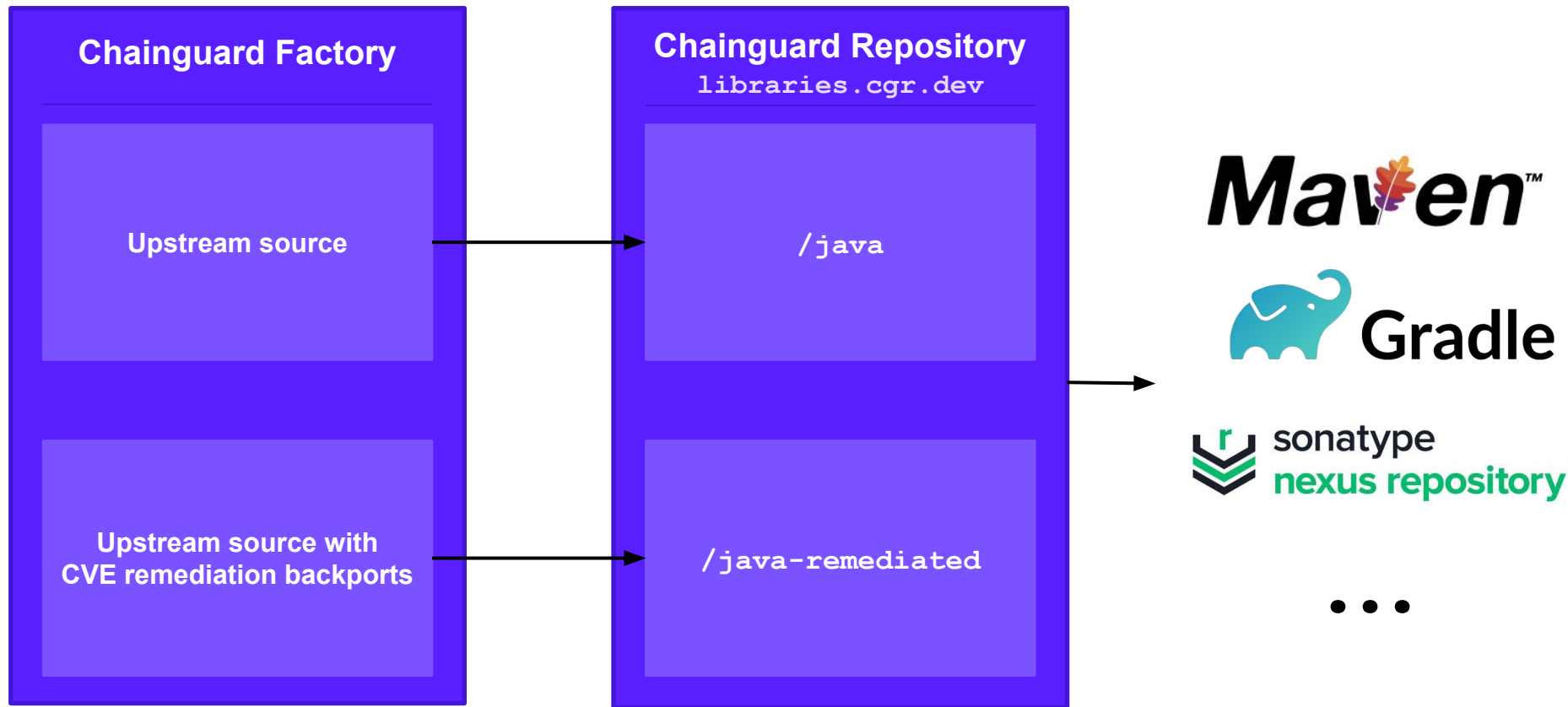
CVE backport process example



BUILD

ACCESS

USE



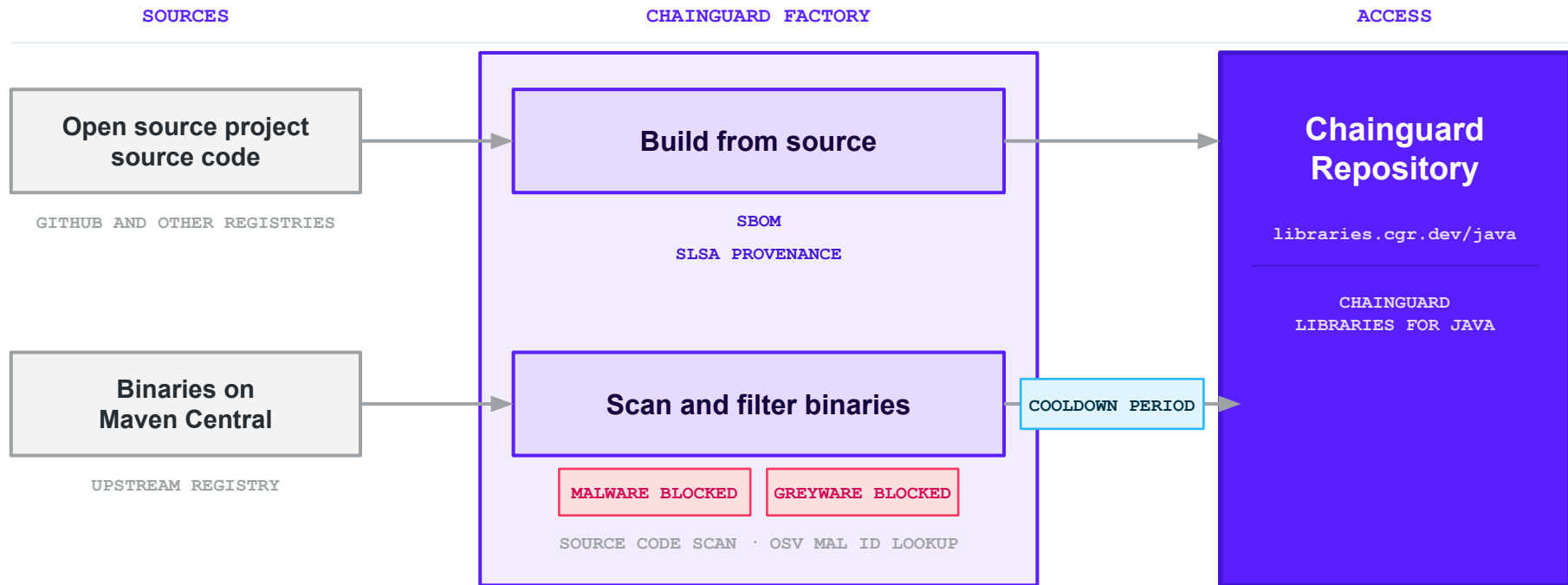
How we decide what to remediate

1	Customer demand	How often is the version downloaded and CVE fixes requested amongst customers?
2	CVE severity	How many critical and high-severity vulnerabilities are there in the version?
3	Viability	Does fixing the CVE cause breaking changes that make a remediation hard to use?
4	Industry scoring coming soon	What are the relevant exploit metrics (CVSS, EPSS, KEV) for the specific CVE?

Let's browse in the console

Fallback and policies

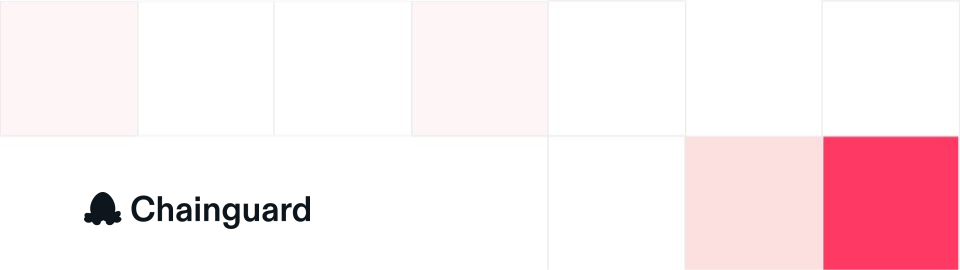
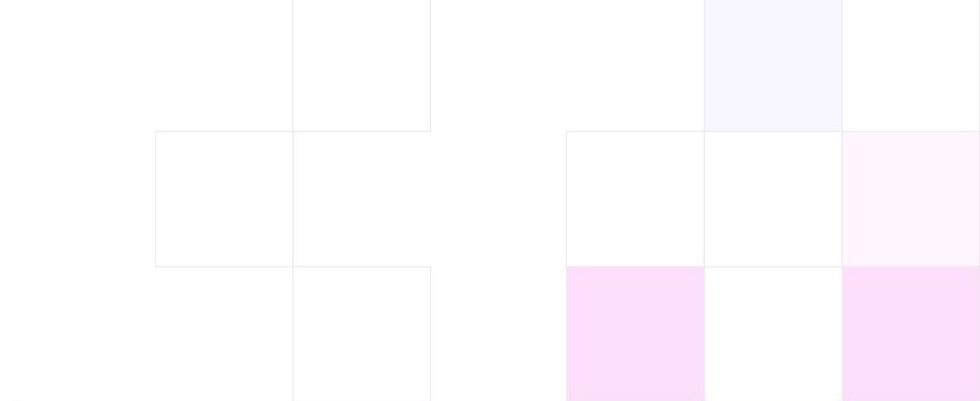
Java fallback and policies



Same pattern for Python (PyPI) and JavaScript (npm)



Demo time



Demo repositories

- <https://github.com/chainguard-demo/chainguard-libraries-java>
- <https://github.com/chainguard-demo/chainguard-libraries-javascript>
- <https://github.com/chainguard-demo/chainguard-libraries-python>

Demos

- **chainctl**
 - **auth, entitlements, policies,...**
- **Manual download scripts**
- **Spring CVE demo with Maven**
 - **settings.xml**
 - **parent**
 - **version properties**
 - **dependencyManagement**

Chainguard Libraries

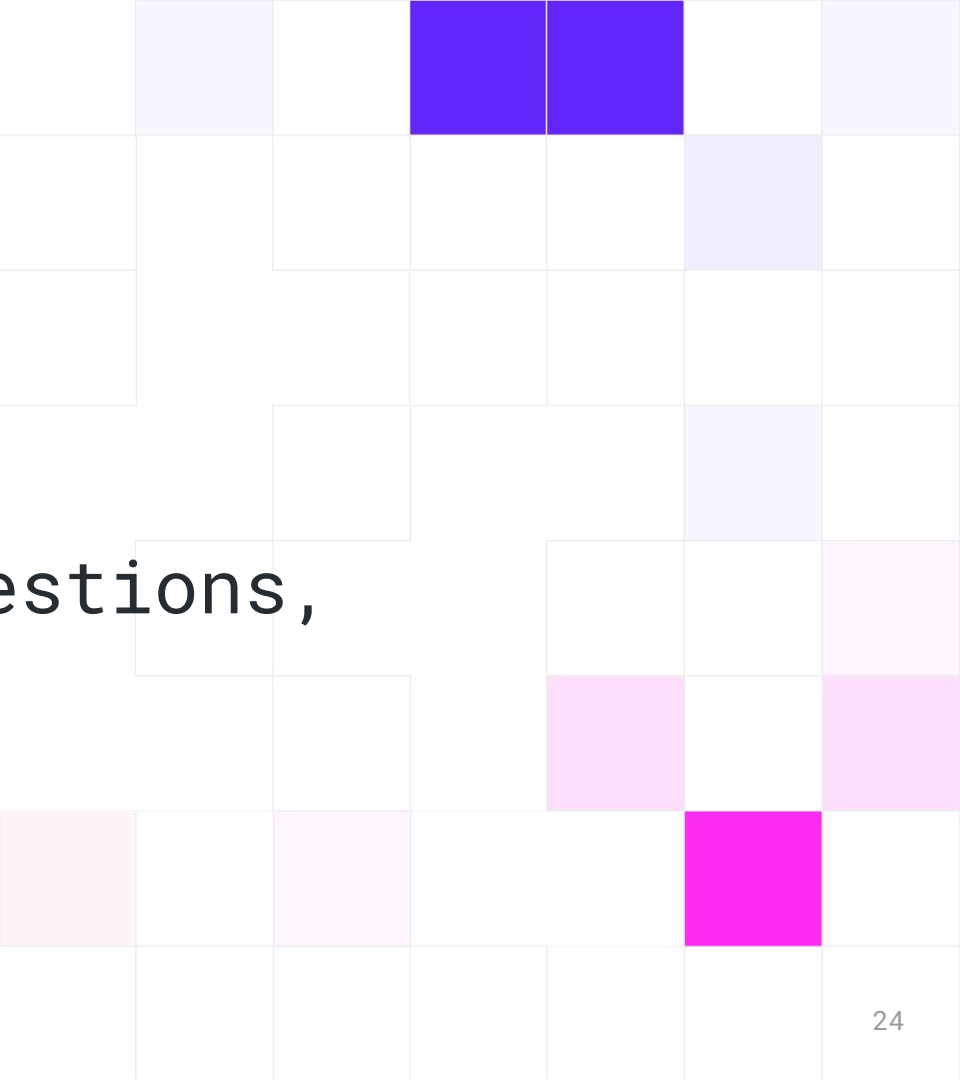


Find out more at
chainguard.dev/libraries



Q&A

There are no bad questions,
so go on and ask.





Thank you

Manfred Moser