chainguard

Learning Lab: Chainguard Libraries for Python

Patrick Smyth

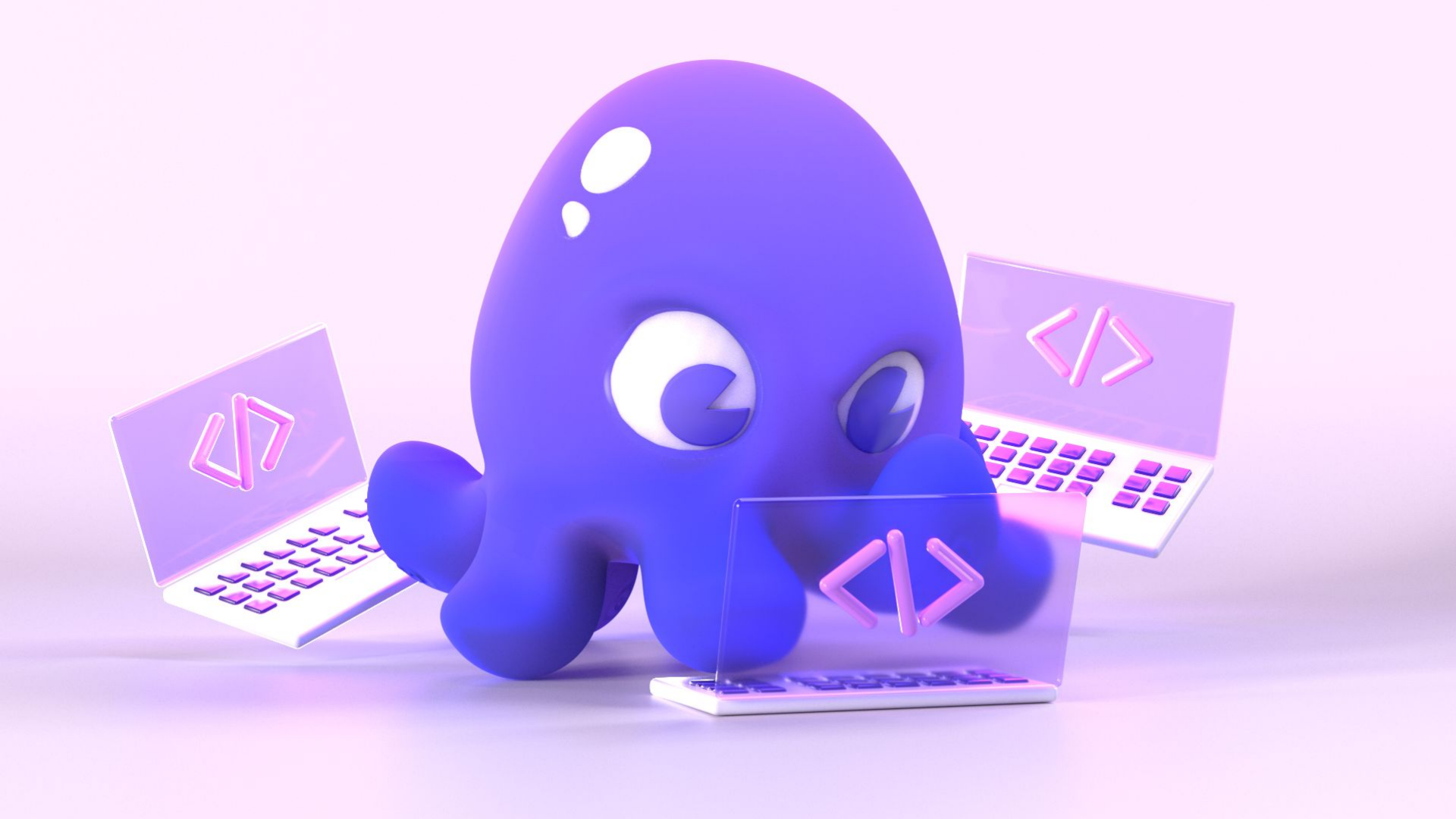
Queens, New York

Staff DevRel at Chainguard

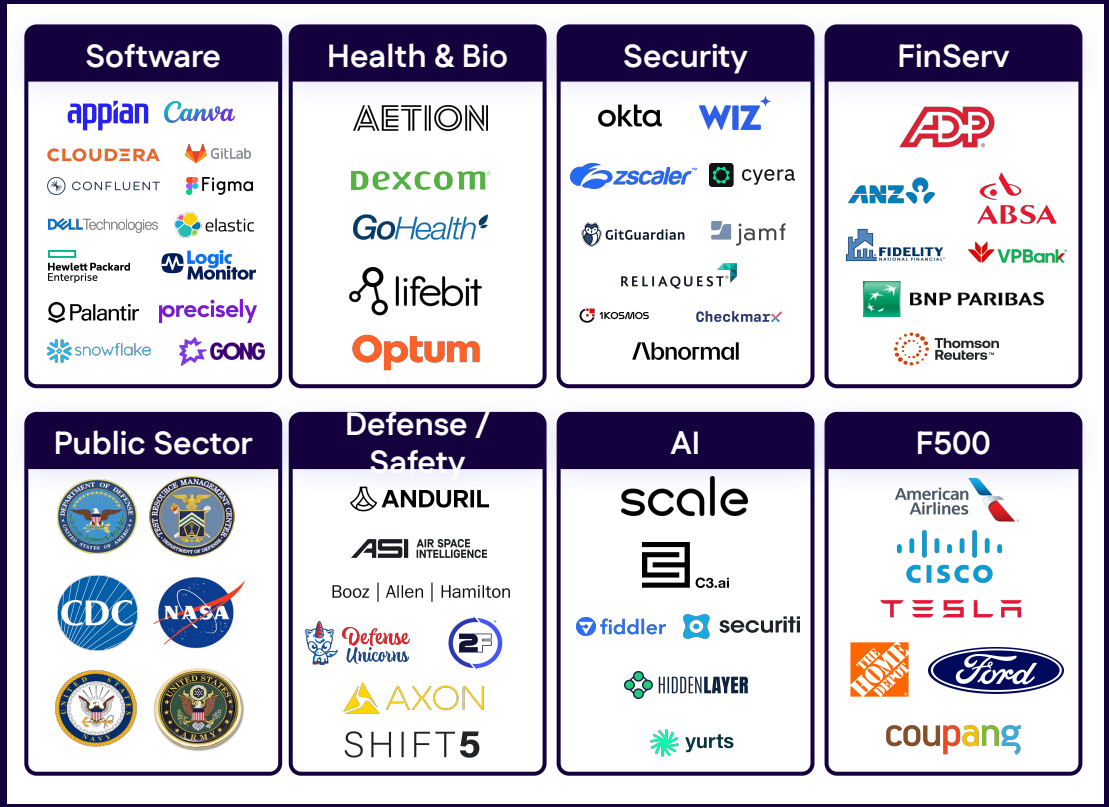
Python, Data Science at
James Webb, Columbia

patrick.smyth@chainguard.dev

@psmyth01 on X

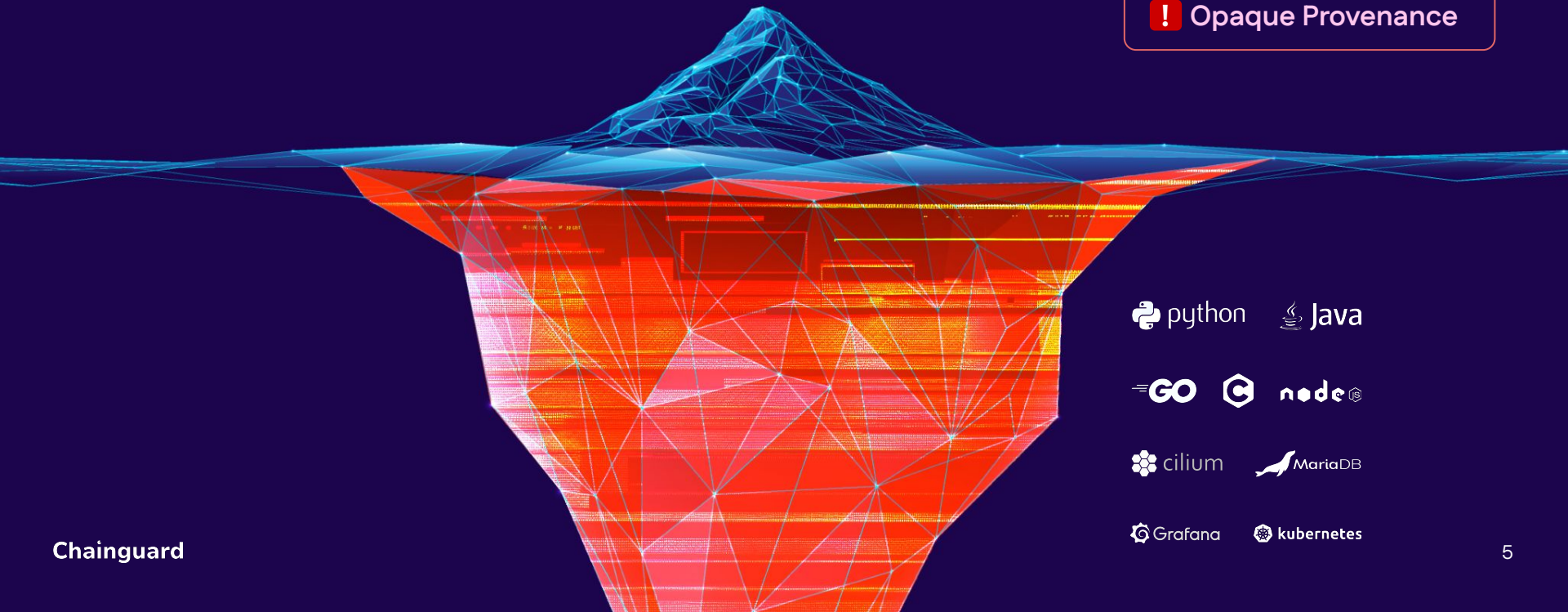


Safe Source for Open Source



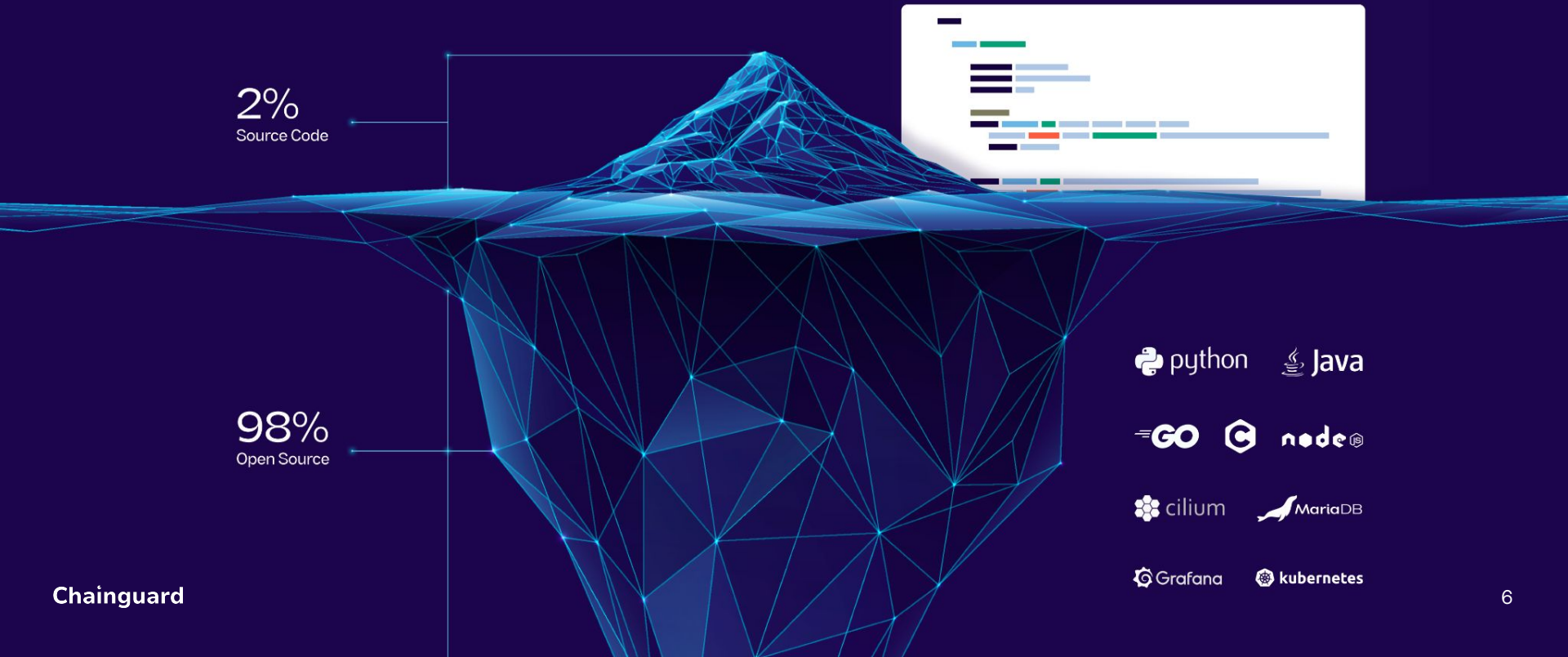
Chainguard Containers

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

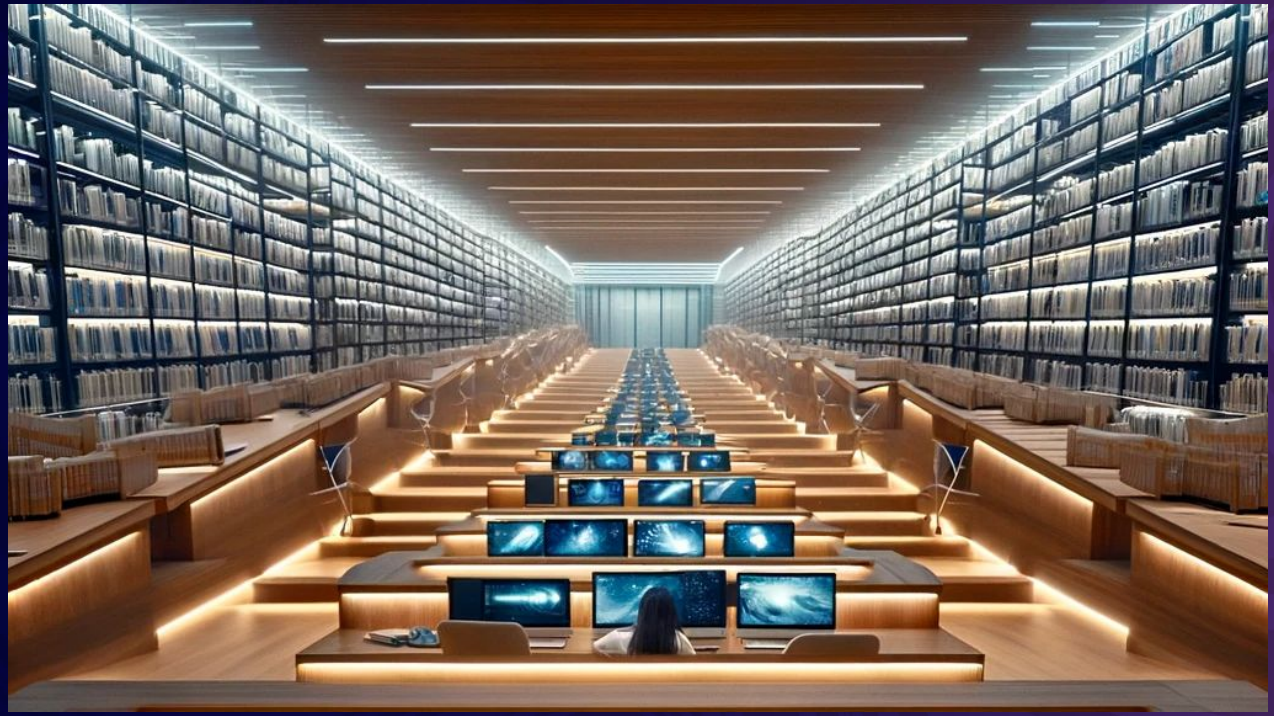


python Java GO C node.js cilium MariaDB Grafana kubernetes

Chainguard Containers



What's a Library?



Transitive Dependencies

What is PyPI?

PyPI / Warehouse

- 634,879 projects
- 1,580,910,735 daily downloads
- 27.4 TB
- Checked 5/12/25

We Got a Problem

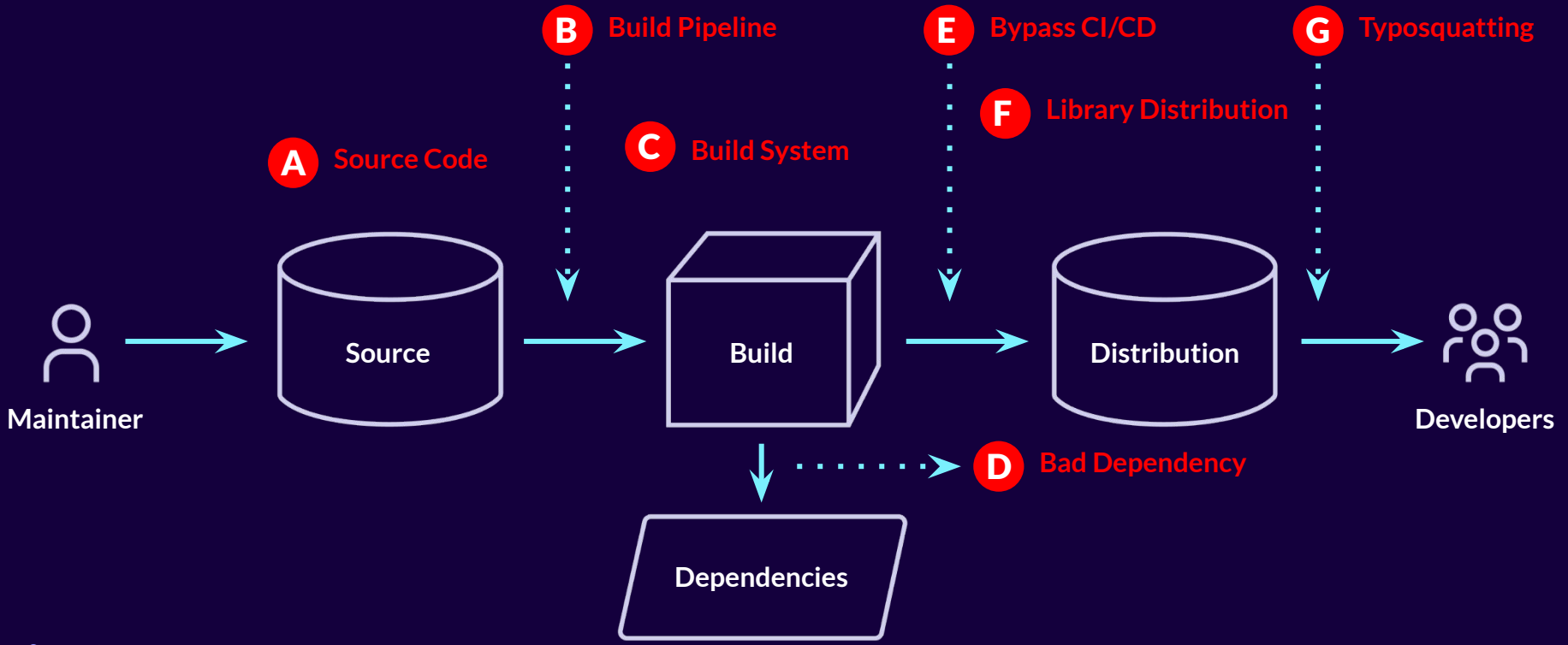
Attack Every Month

Software Supply Chain Speedrun

- Raw materials to finished product
- Complex network
- Many actors, many steps

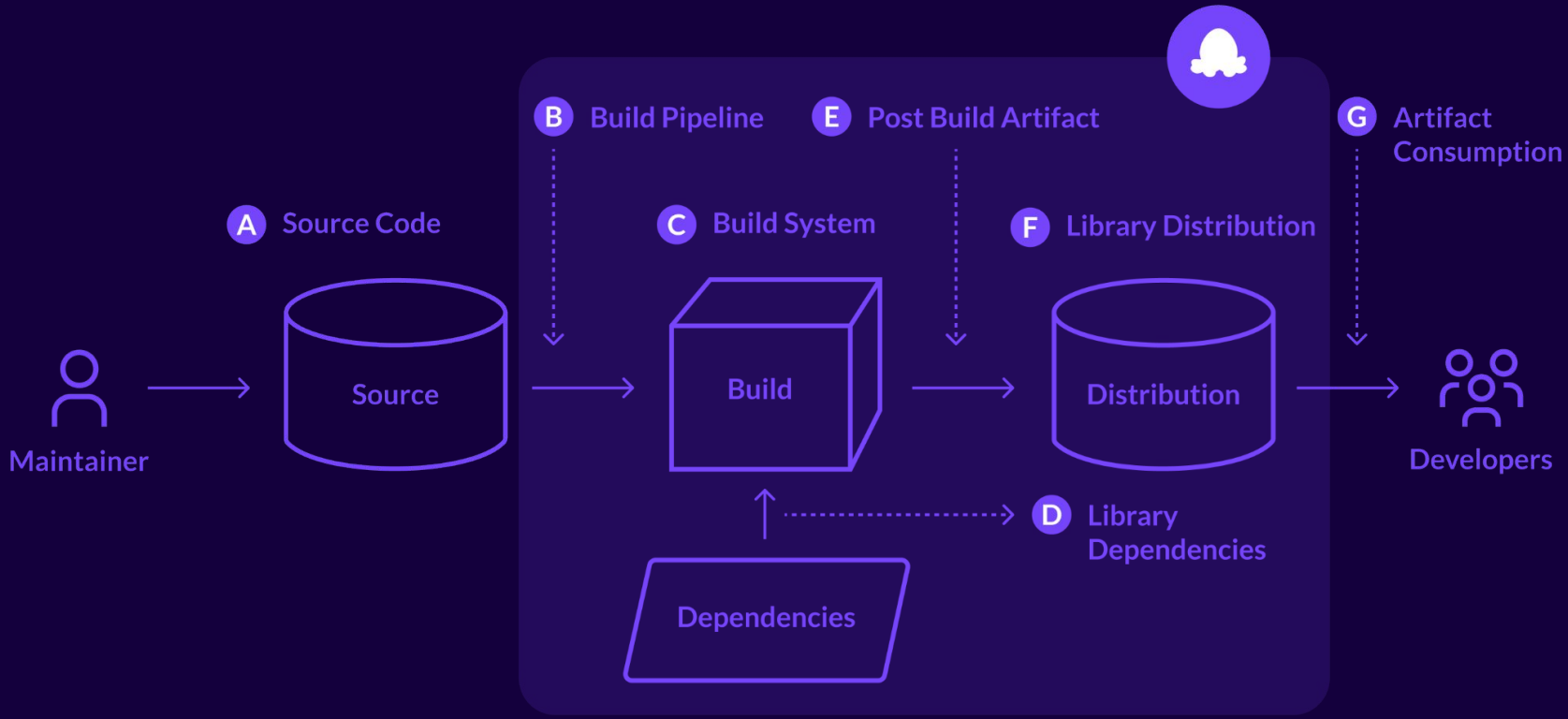
Stuff Flows Downhill

Points of Failure

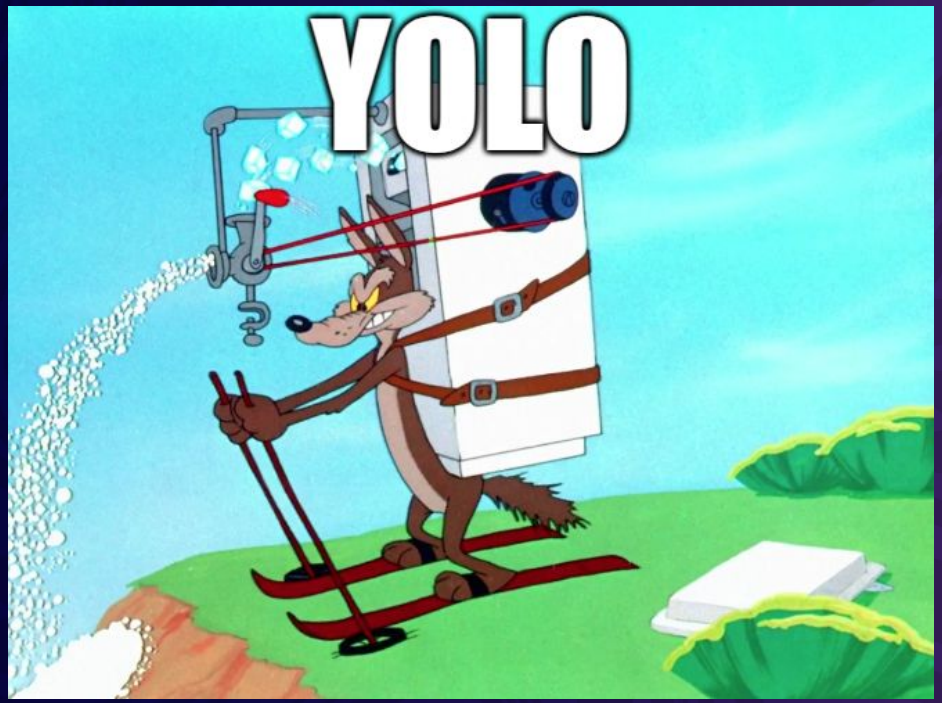


Chainguard Libraries

Source > Chainguard Factory > You



Ultralytics YOLO Attack



Chainguard Factory

Chainguard Factory

- What is it?
- Fitting into the supply chain landscape
- Python ecosystem and Dark Matter

DEMO

Chainguard Libraries

chainguard.dev/libraries

chainguard


Goodbye!