chainguard

Learning Lab: Chainguard Libraries for Python

Patrick Smyth

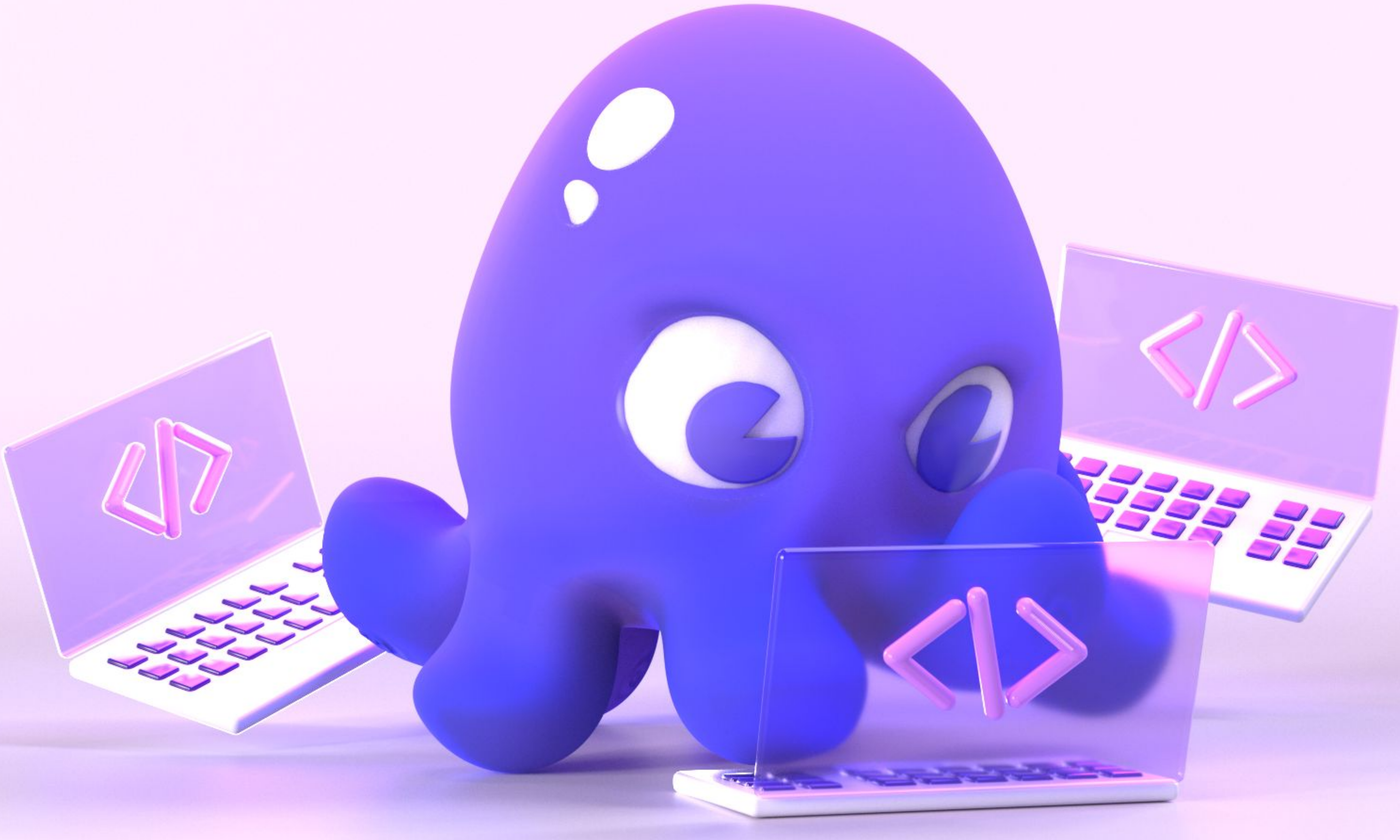
Queens, New York

Staff DevRel at Chainguard

Python, Data Science at
James Webb, Columbia

patrick.smyth@chainguard.dev

@psmyth01 on X



Safe Source for Open Source

Software

appian Canva
CLOUDERA GitLab
CONFLUENT Figma
DELL Technologies elastic
Hewlett Packard Enterprise LogicMonitor
Palantir precisely
snowflake GONG

Health & Bio

AETION
dexcom
GoHealth
lifebit
Optum

Security

okta WIZ
zscaler cyera
GitGuardian jamf
RELIAQUEST
1KOSMOS Checkmarx
Abnormal

FinServ

ADP
ANZ ABSA
FIDELITY NATIONAL FINANCIAL VPBank
BNP PARIBAS
Thomson Reuters

Public Sector

Department of Defense United States of America
Test Resource Management Center Department of Defense
CDC NASA
United States Navy
United States Army

Defense / Safety

ANDURIL
ASI AIR SPACE INTELLIGENCE
Booz | Allen | Hamilton
Defense Unicorns 2F
AXON
SHIFT5

AI

scale
C3.ai
fiddler securiti
HIDDENLAYER
yurts

F500

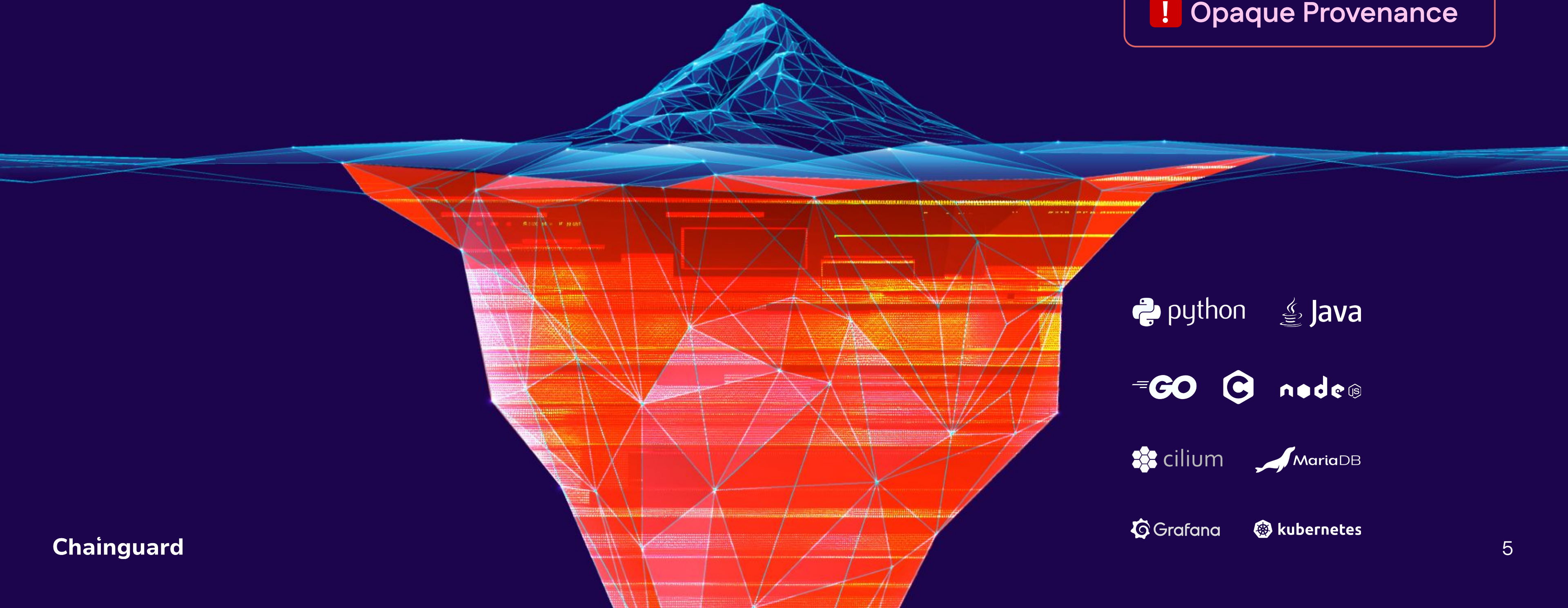
American Airlines
CISCO
TESLA
THE HOME DEPOT Ford
coupang

Chainguard Containers

❗ Persistent CVEs

❗ Large Attack Surface

❗ Opaque Provenance



python Java

GO C node JS

cilium MariaDB

Grafana kubernetes

Chainguard Containers

2%
Source Code

98%
Open Source

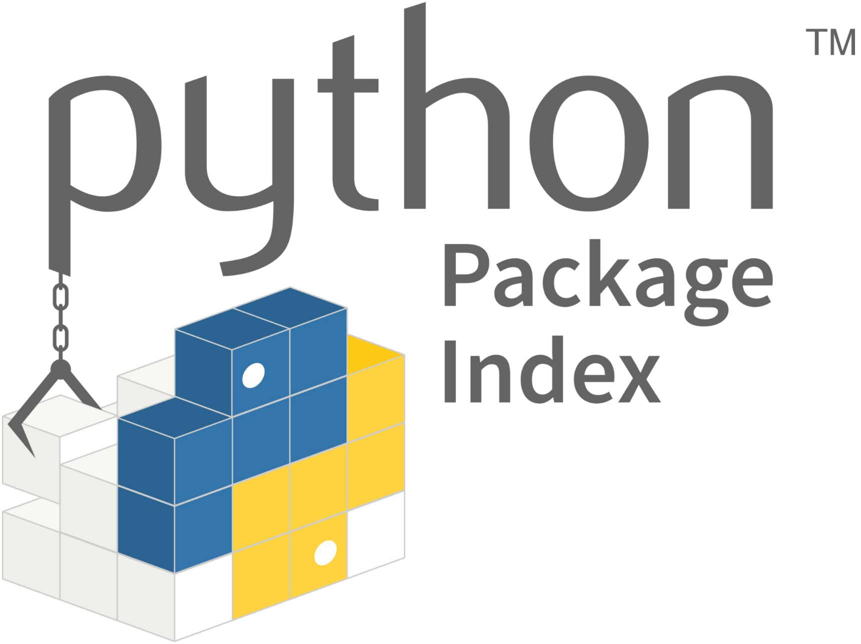
python
Java
GO
C
node JS
cilium
MariaDB
Grafana
kubernetes

What’s a Library?

Transitive Dependencies

What is PyPI?

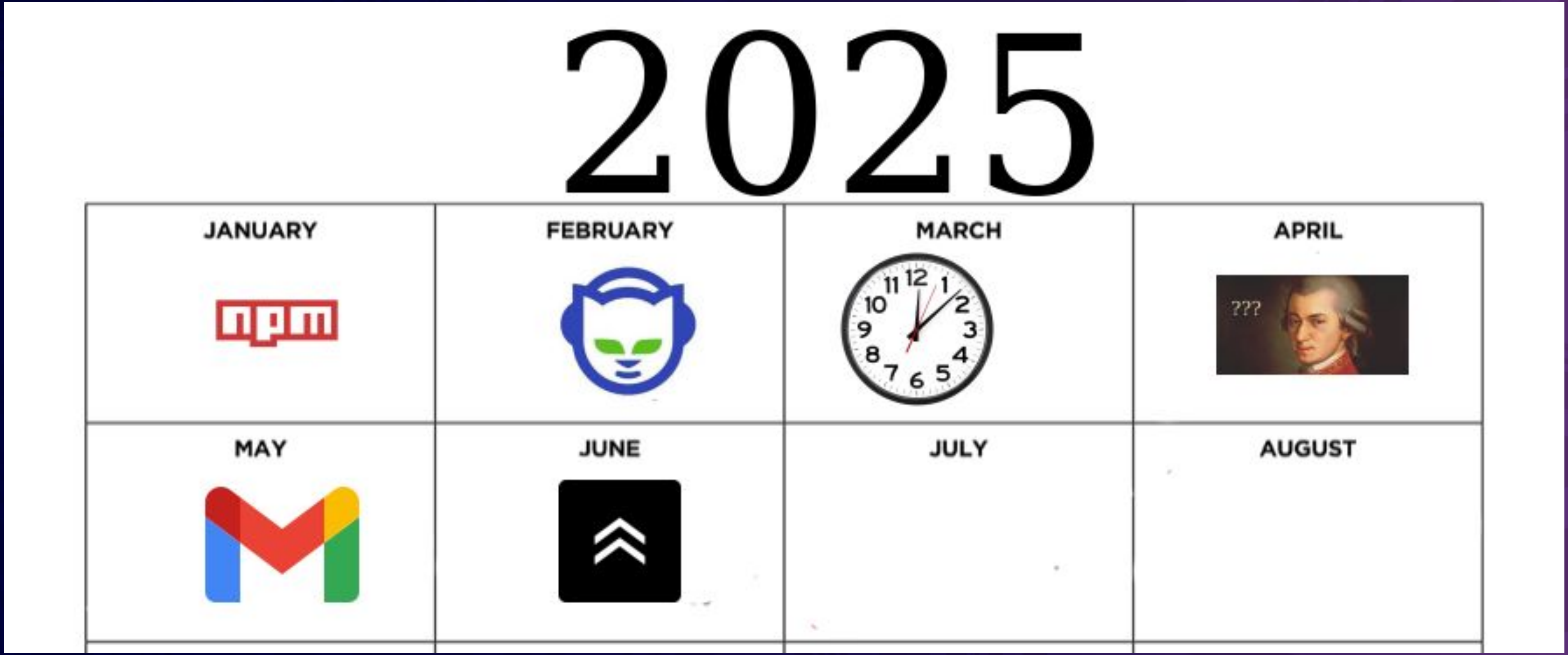
PyPI / Warehouse



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

We Got a Problem

Attack Every Month



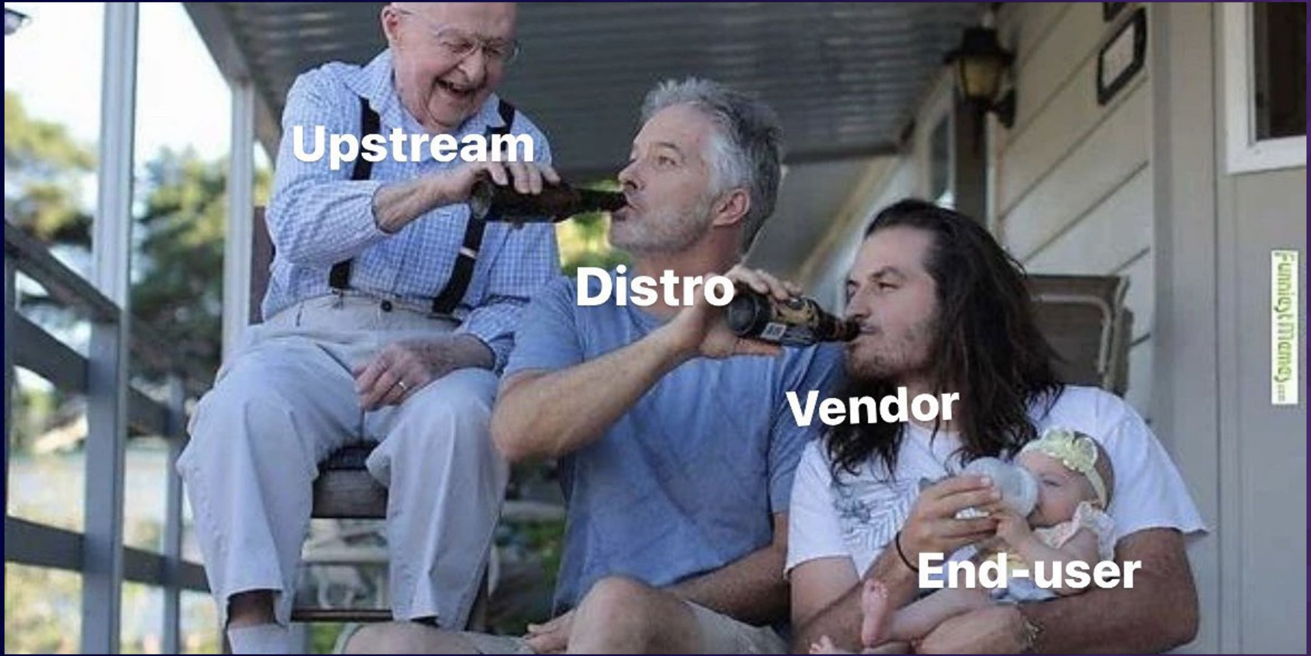
2025

JANUARY	FEBRUARY	MARCH	APRIL
MAY	JUNE	JULY	AUGUST

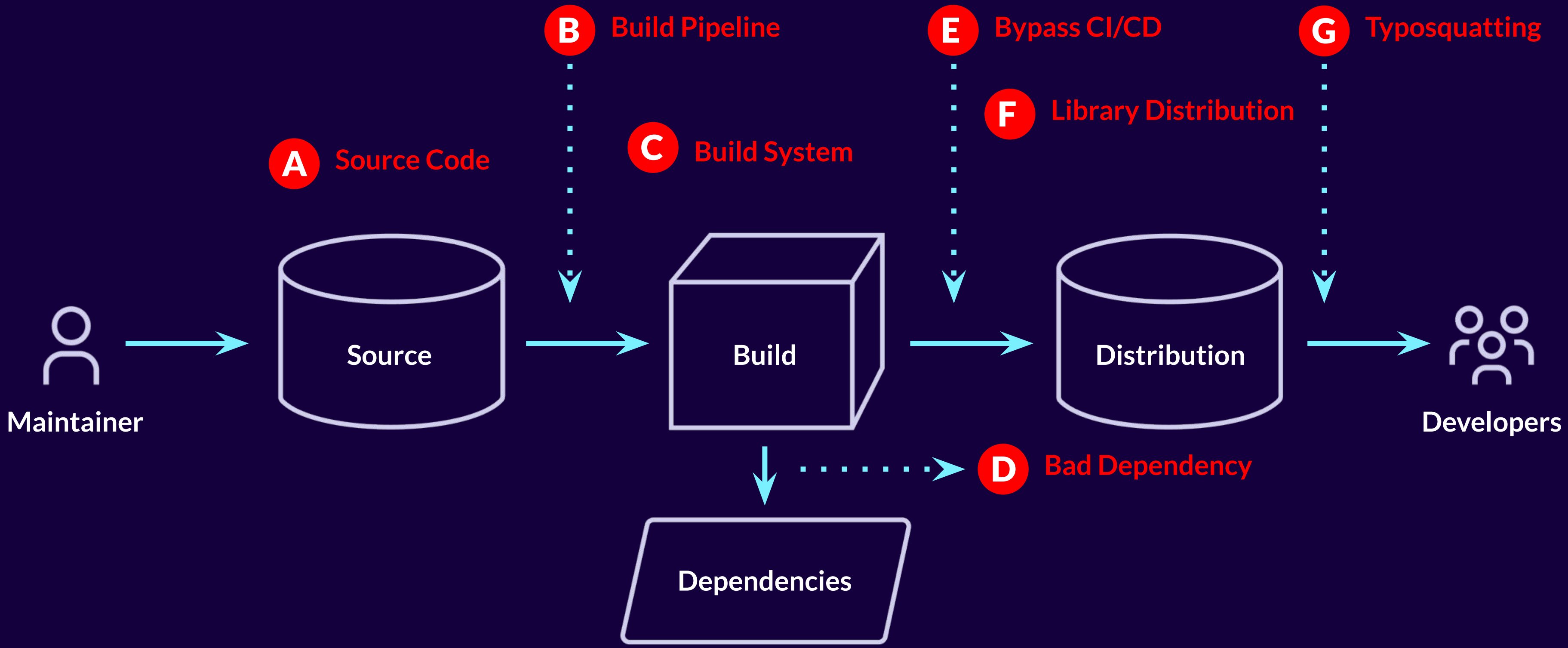
Software Supply Chain Speedrun

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

Stuff Flows Downhill



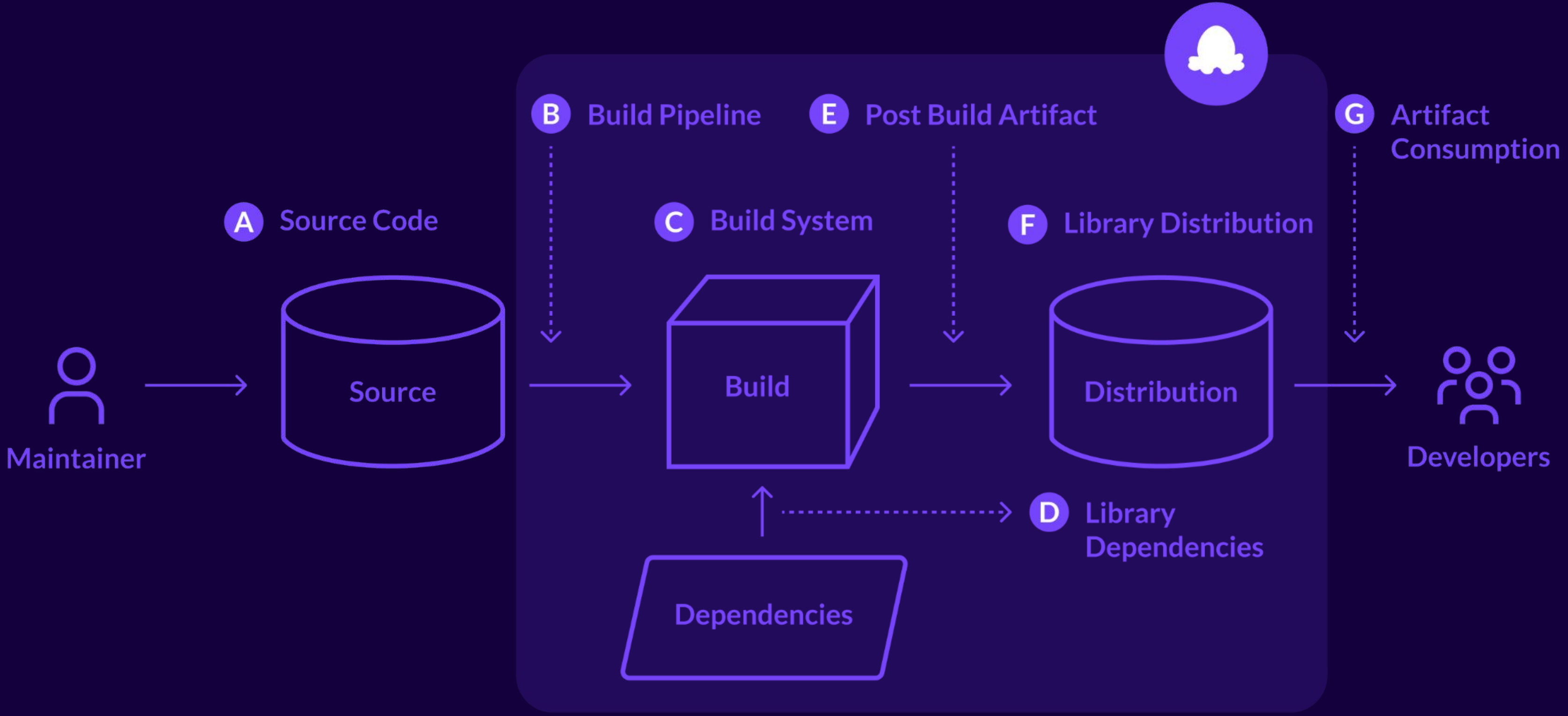
Points of Failure



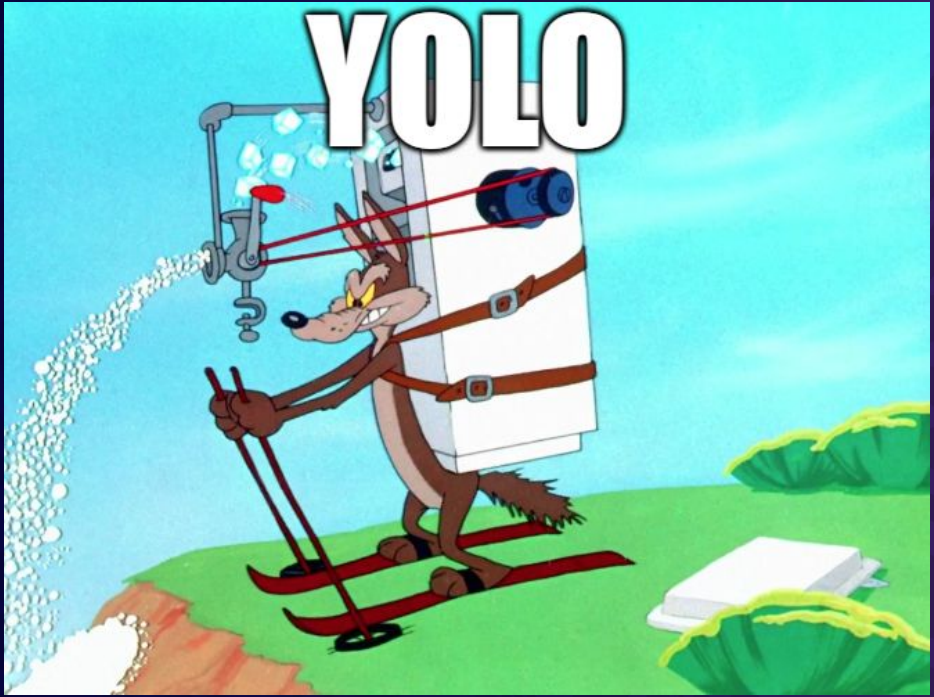
chainguard

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

go.chainguard.dev/ll-python-libraries

Chainguard Libraries

chainguard.dev/libraries

chainguard

Goodbye!