chainguard

Learning Lab: AI with Hardened Container Images

PyTorch

Patrick Smyth

Queens, New York

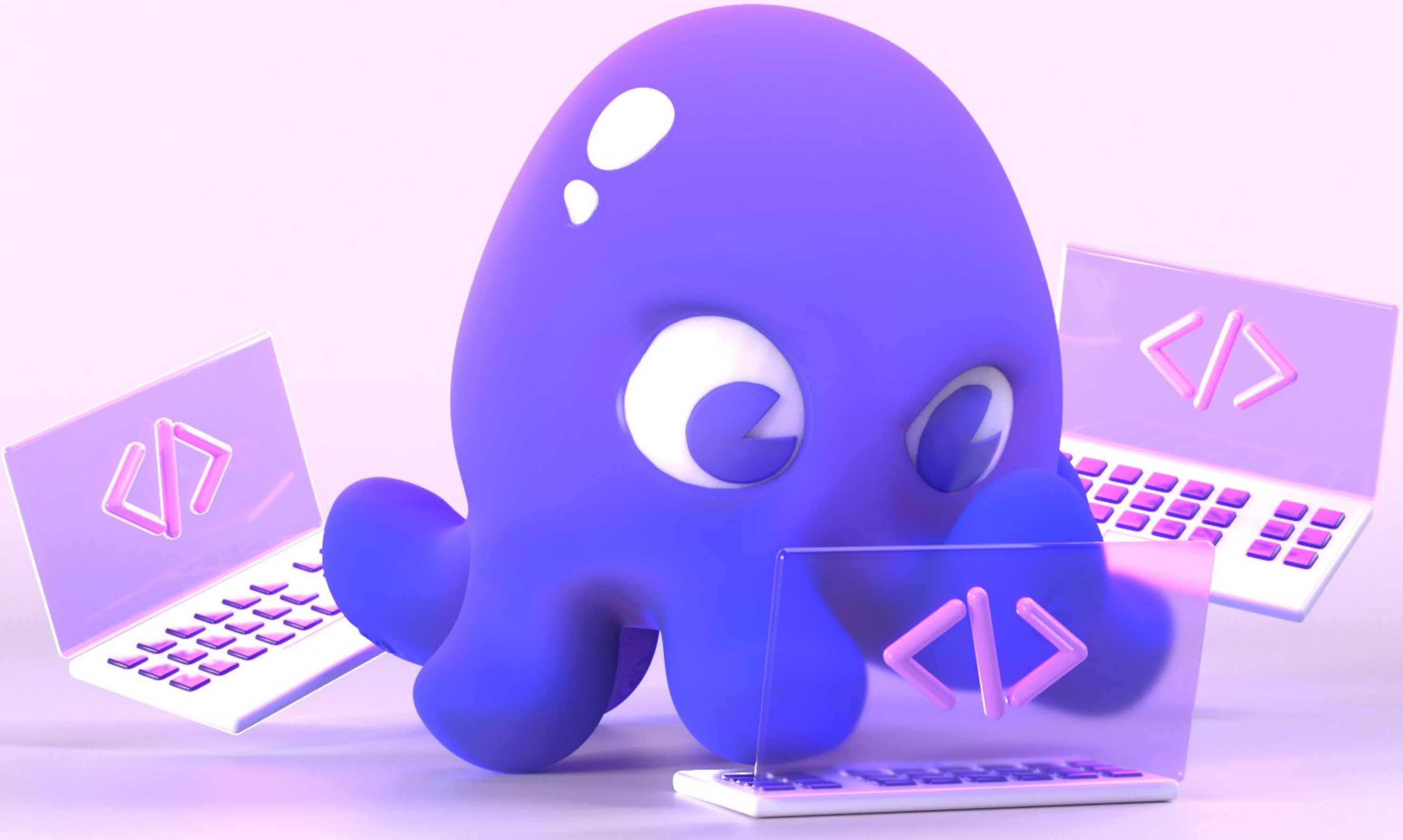
Staff DevRel at Chainguard

Python, Data Science at
James Webb, Columbia

patrick.smyth@chainguard.dev

@psmyth01 on X

```
docker pull cgr.dev/chainguard/pytorch
```



Safe source
For open source

~~Shift~~ Start left

Raise waterline

Hapag-Lloyd

coupang

GitGuardian

nav

BNP PARIBAS

ABSA

AVEVA

Danske Bank

ZAMA

Wealthsimple

Government of Canada

GONG

Cellebrite

SYSTEMATIC

VPBank

Canva

swyftx

Department for Work & Pensions

ANZ

Everllence

nationwide

trivago

Trustpilot

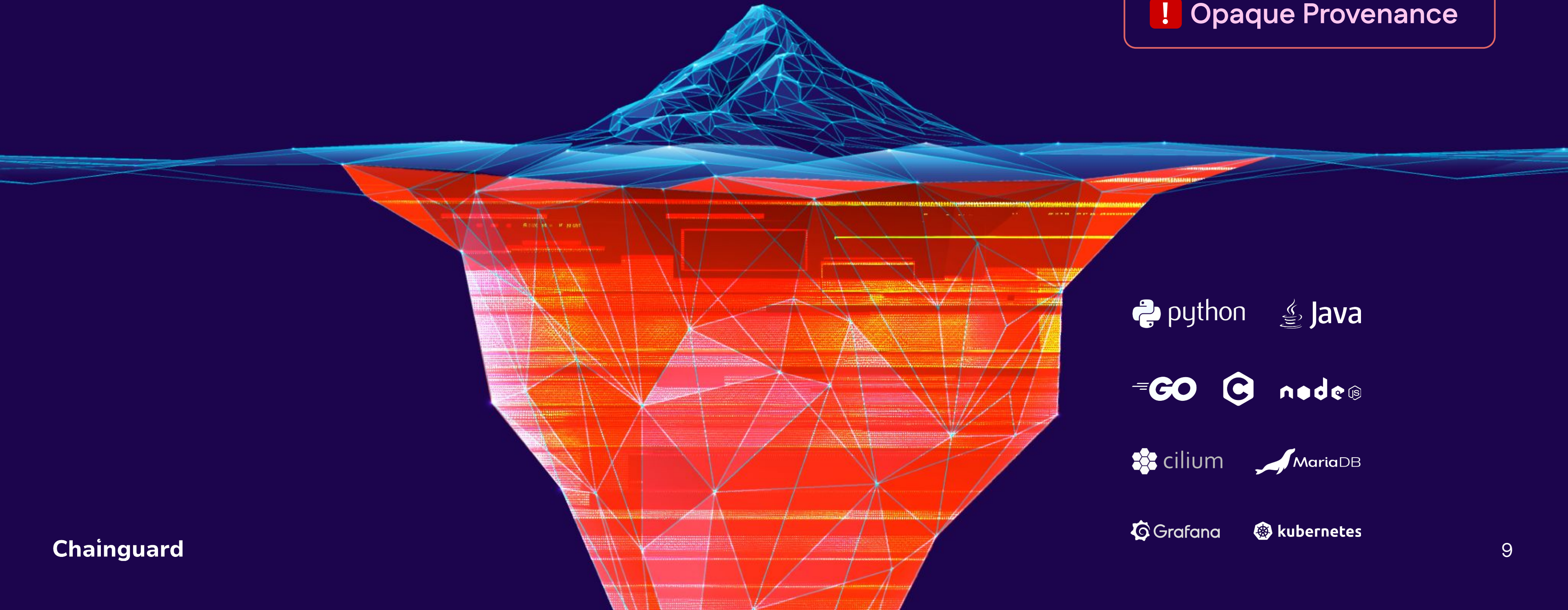
chainguard

CVE System

YOUR APP
CVEs

Boss assigned me
TO FIX UBUNTU

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



python Java

GO C node JS

cilium MariaDB

Grafana kubernetes

2%
Source Code

98%
Open Source

python
Java
GO
C
node JS
cilium
MariaDB
Grafana
kubernetes

The scanner is reading
0 CVEs!

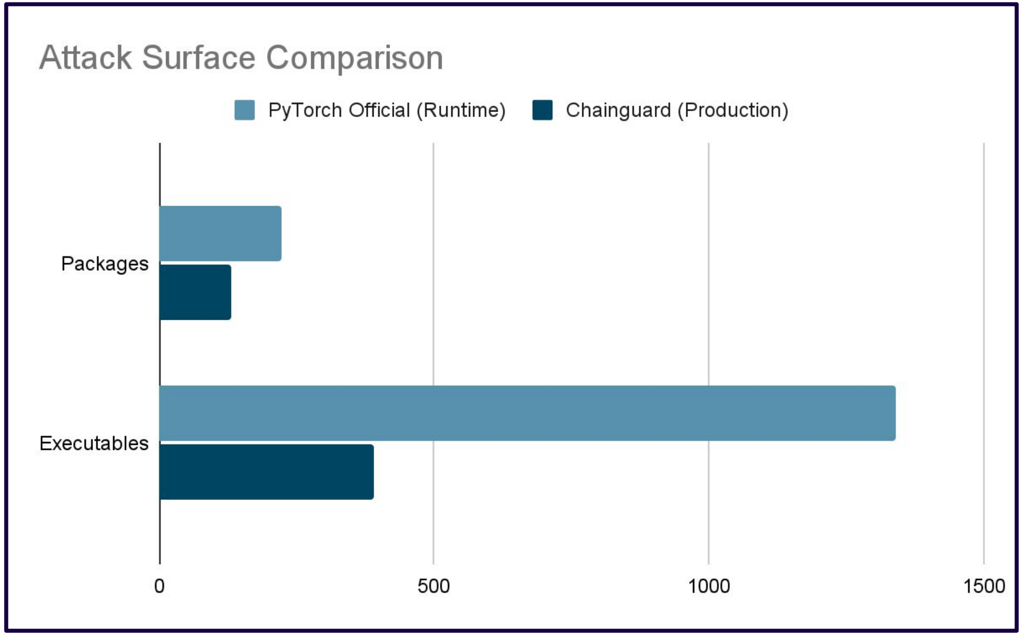
TOIL.

How We Do It

AI CONTAINERS
CONTAINERS
imgflip.com

Have you seen...

Attack Surface Comparison

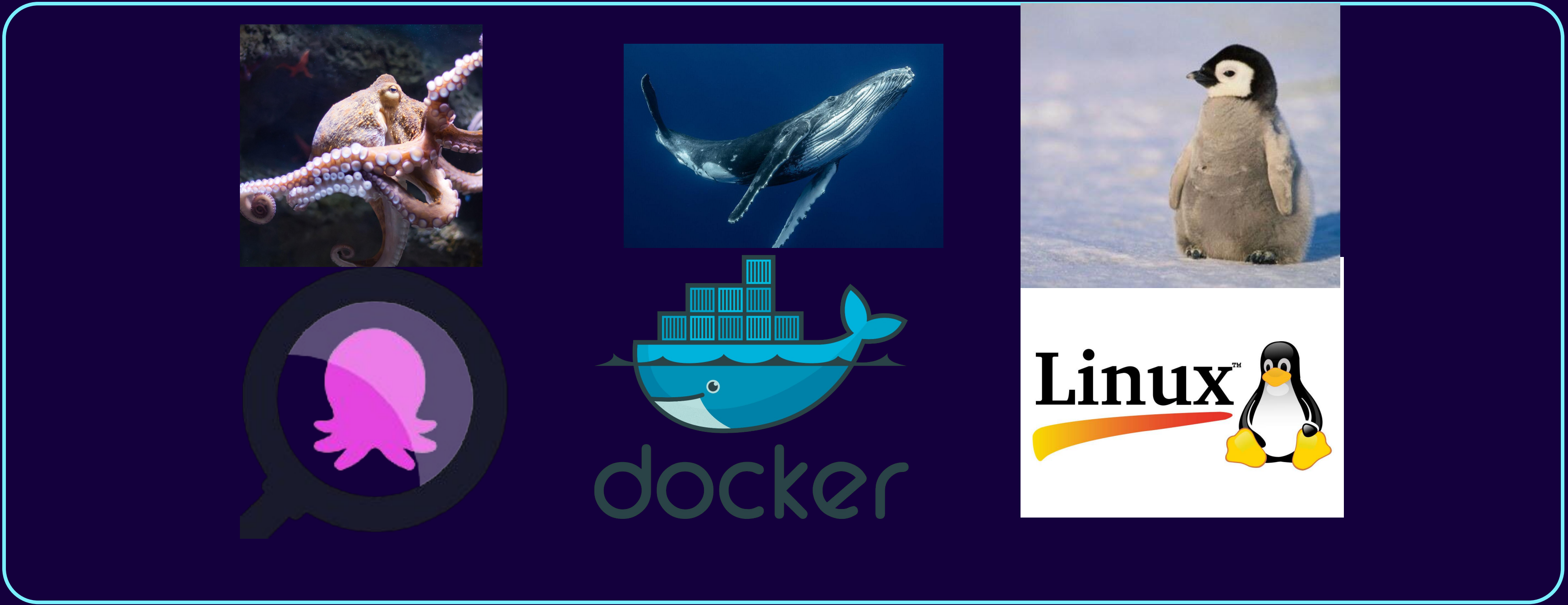


chainguard

DEMO

go.chainguard.dev/ai-ll

IMAGE CLASSIFICATION



Chainguard Libraries

get.chainguard.dev/ai-images

Goodbye!