chainguard

Software Supply Chain Security

DataDog + Chainguard at Boston CSA

Patrick Smyth

Queens, New York

Staff DevRel at Chainguard

Python, Data Science at
James Webb, Columbia

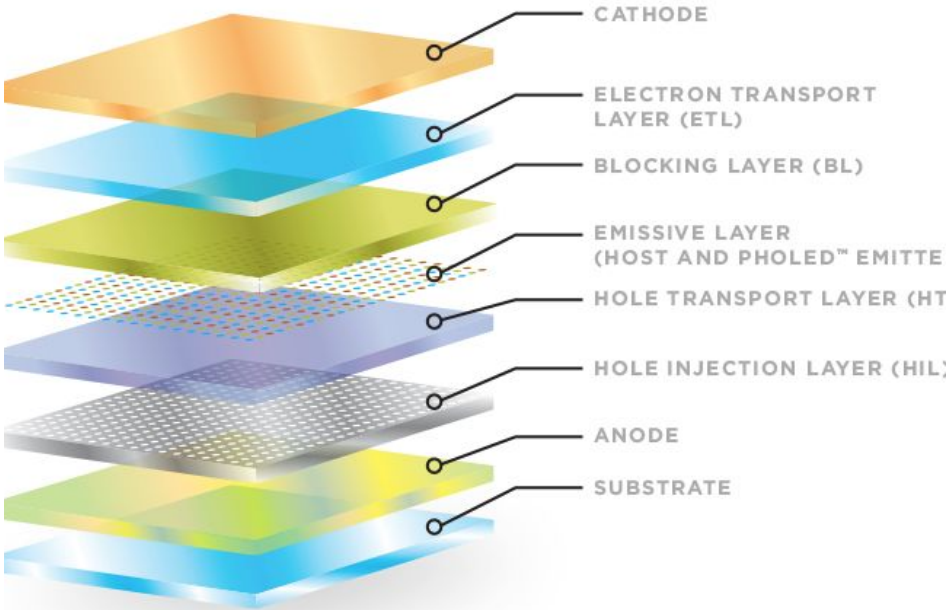
patrick.smyth@chainguard.dev

@psmyth01 on X

Physical Supply Chain

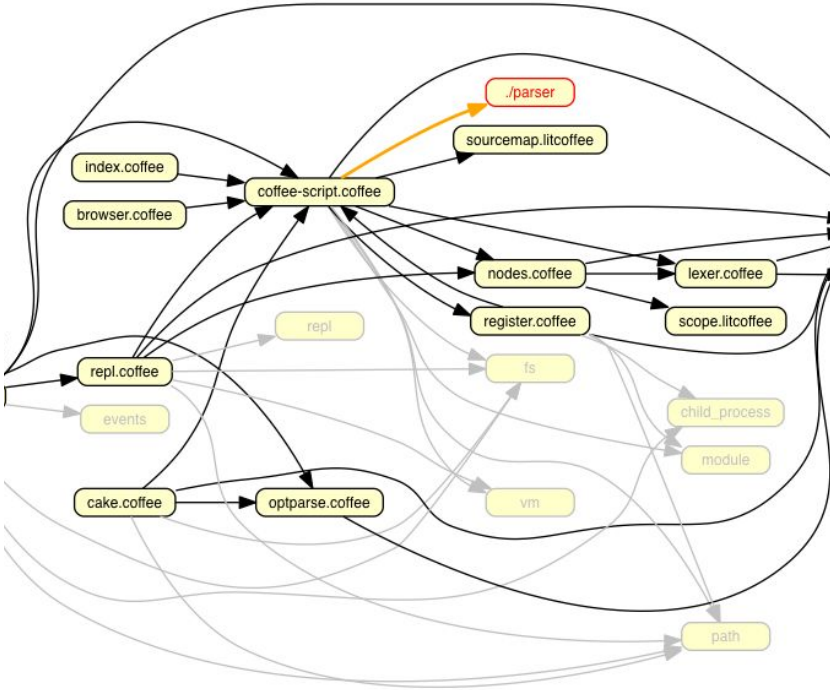
- Raw materials to finished product
- Complex network
- Many actors, many steps

Interdependence



Transitive Dependencies

Software Supply Chain



- Software built on other software
- “Dependencies”
- Dependencies have dependencies

“Shift” Flows Downhill

Not Just Application Deps, sorry :(

CVE System


YOUR APP
CVEs

Who Tracks CVEs?

Who Tracks CVEs?

MITRE

Incidents

Solar Winds (90s Shareware on Floppy)

Solar Winds (OG Supply Chain Hack)

CVE-2022-0847

“Dirty Pipe”

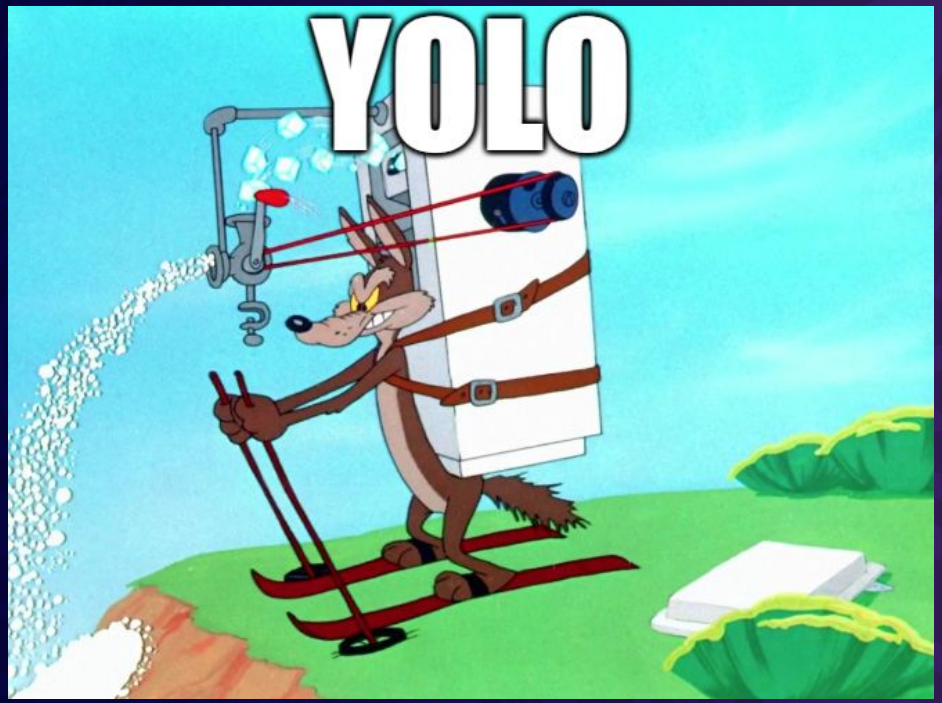
- Linux Kernel vulnerability
- Write to read-only files
- Privilege escalation
- Android devices affected
- “Catastrophic”

CVE-2021-44228

“Log4Shell”

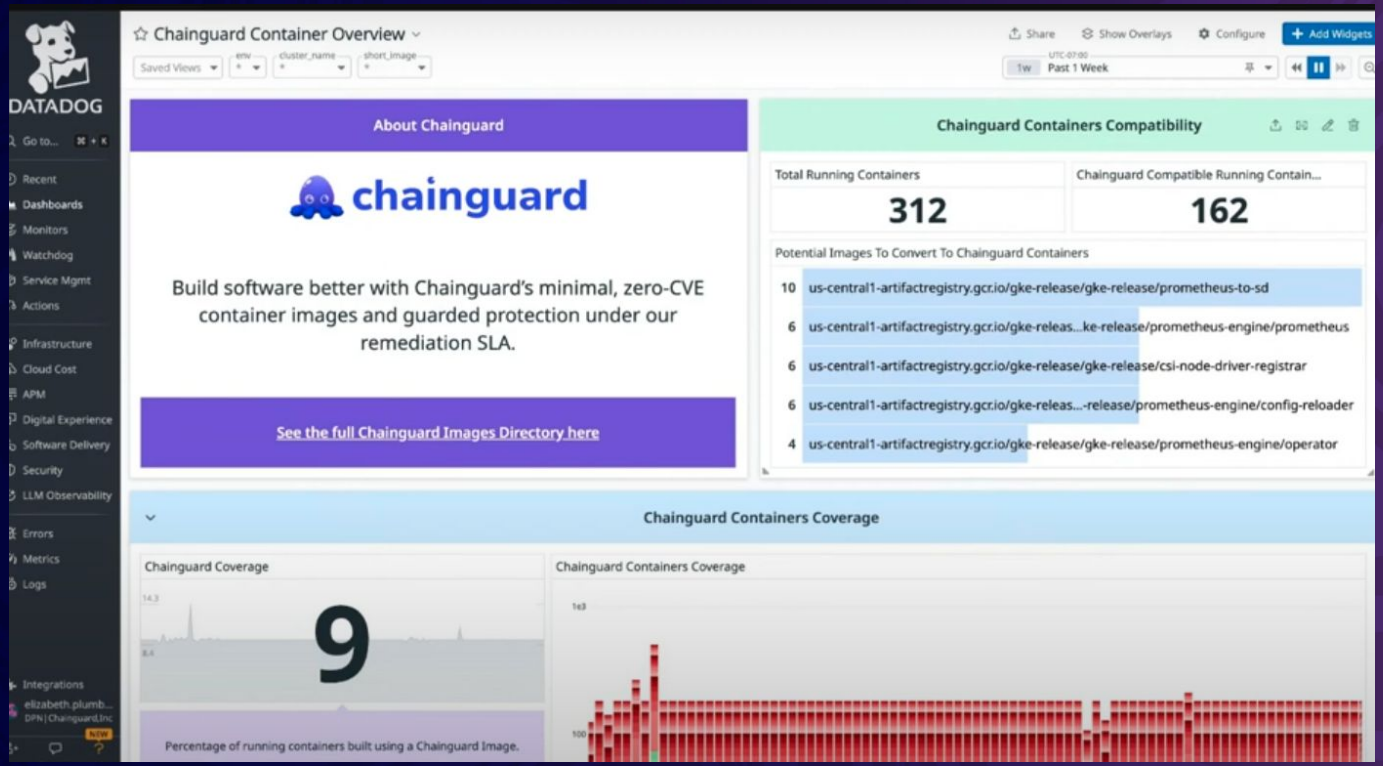
- Arguably worst vulnerability of all time
- Attempted attacks on over 40% of world business networks
- Hundreds of millions of devices vulnerable

YOLO! (Ultralytics YOLO Attack)



SLSA

Observability (DataDog +Chainguard)



Chainguard Libraries

Chainguard Factory

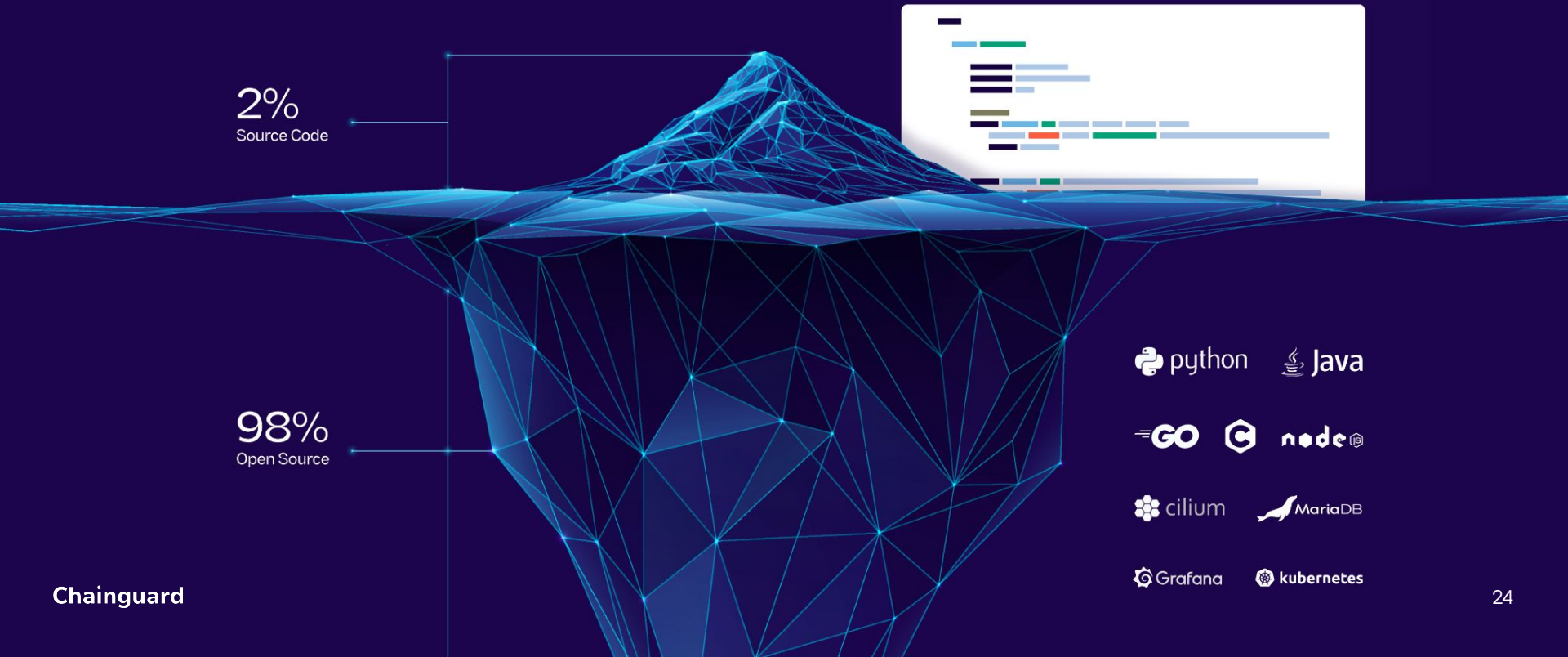
Scanners

aqua trivy

grype

snyk

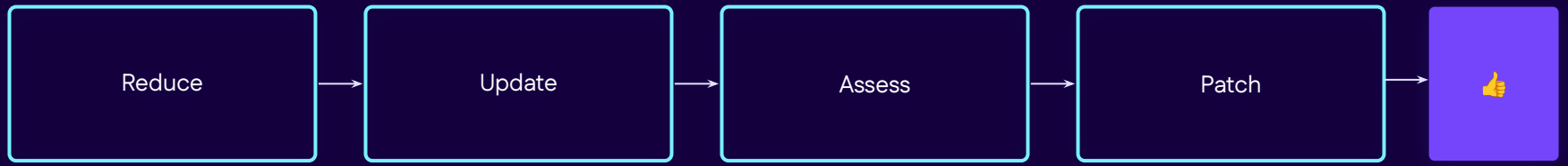
Open Source Software Has Transformed Software Development



DEMO TIME

Follow along on
go.chainguard.dev/introduction-supply-chain-demo

Software Supply Chain Security Principles



Resources

- *NIST SP 800-161r1-upd1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*
- *NIST Special Publication 800-53 / Risk Assessment (RA)*
- *Cybersecurity Supply Chain Risk Management C-SCRM*
- *Security and Privacy Controls for Information Systems and Organizations*
- *MITRE ATT&CK*


Goodbye!