
Building a Secure,
Automated Supply Chain
Workshop


https://andyc.info/dc19

Please:

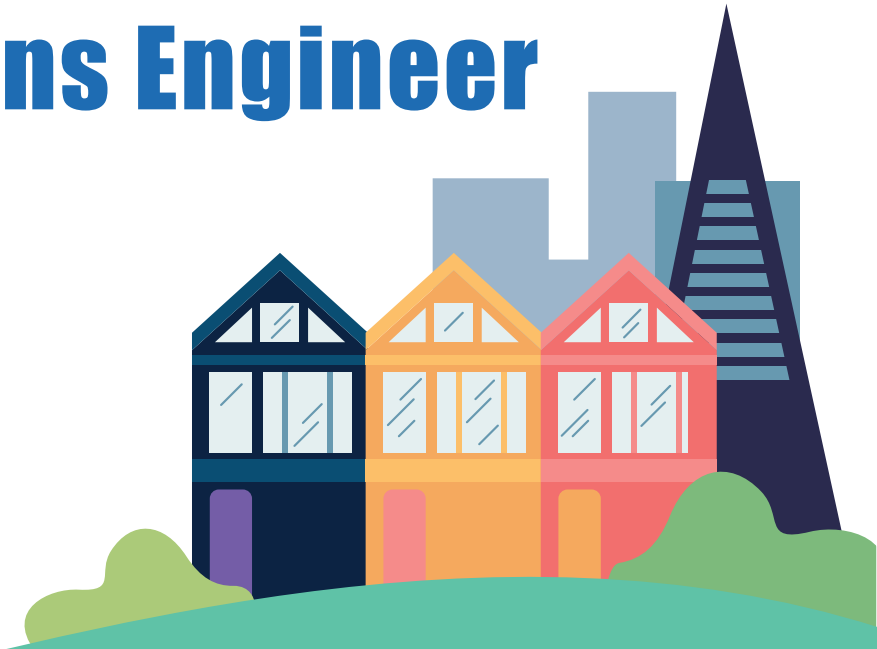
- Ask Questions
- Help each other
- Take breaks as needed
- Have fun
- Learn
- There will be prizes!

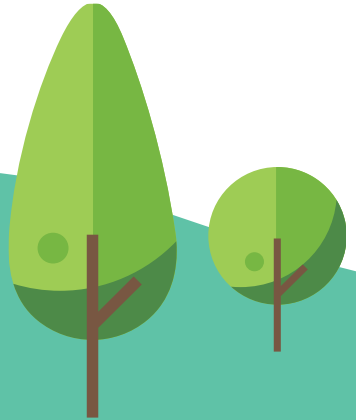
Andy Clemenko

Senior Solutions Engineer

Docker Inc

@clemenko





Dad
Geek
Cyclist
Firefighter
6th Dockercon!

What is NOT a Secure Supply Chain?

What is a Secure Supply Chain?

- Known good source - Source of truth?
- Known good path?
- CVE Scanned?
- Repeatable?
- Chain of Custody (Audit Trail)?

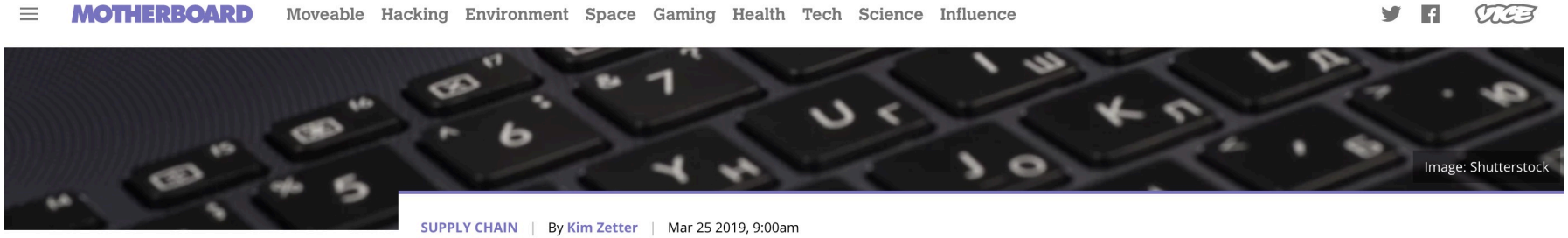
Why?

Honestly Why?

Have you seen my thumb drives?

#dockercon19supplychainattack

Anyone have an Asus Laptop?



SUPPLY CHAIN | By Kim Zetter | Mar 25 2019, 9:00am

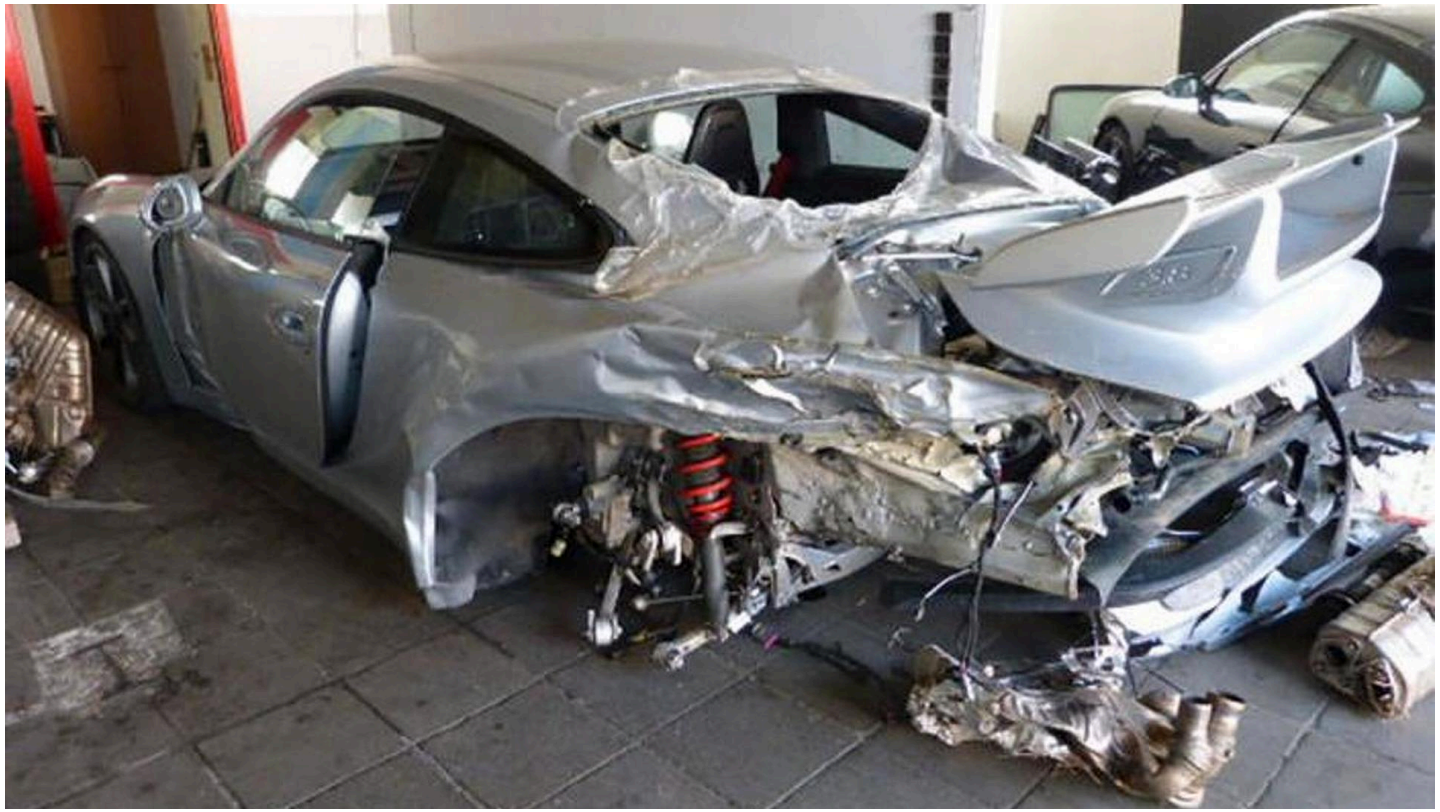
Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers

https://andyc.info/asus

Man in the Middle?

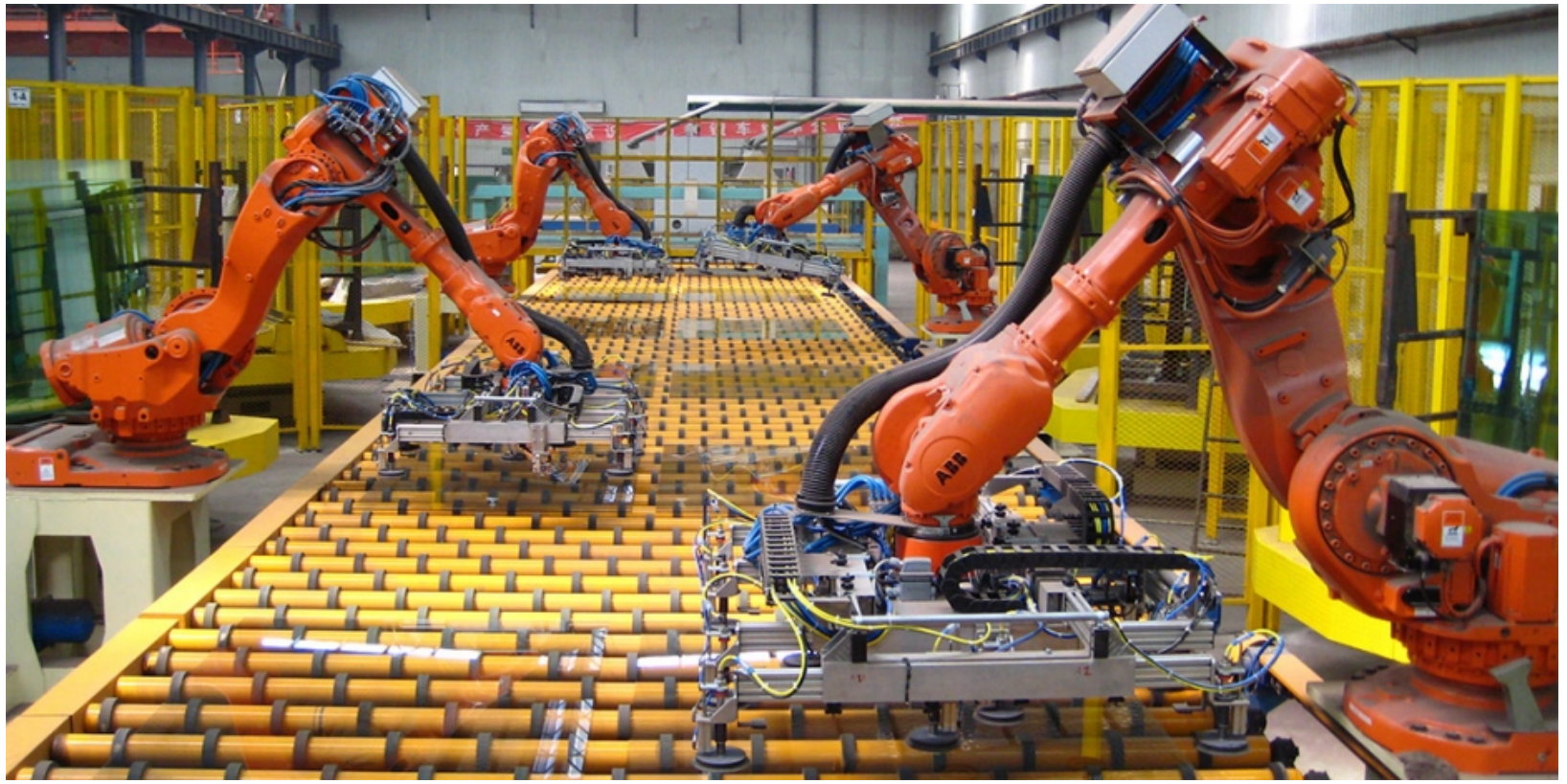
Docker pull from 35k feet!

Replay Attack?



Automation = Vacations!

Automation = Repeatability



Vulnerabilities?

34 minutes ago
by admin

34 critical 241 major 2 minor

20 hours ago
by admin

32 critical 224 major 2 minor

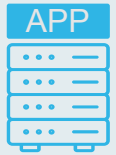
Scan out of date Retry

Chain of Custody?

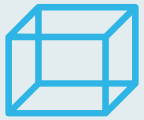
“No human should EVER build or deploy code meant for production!”

Image credit: https://www.deviantart.com/uvnik/art/No-humans-allowed-142046016

Images for everything!

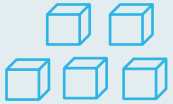


TRADITIONAL APPS



PACKAGED APPS

NEW APPS



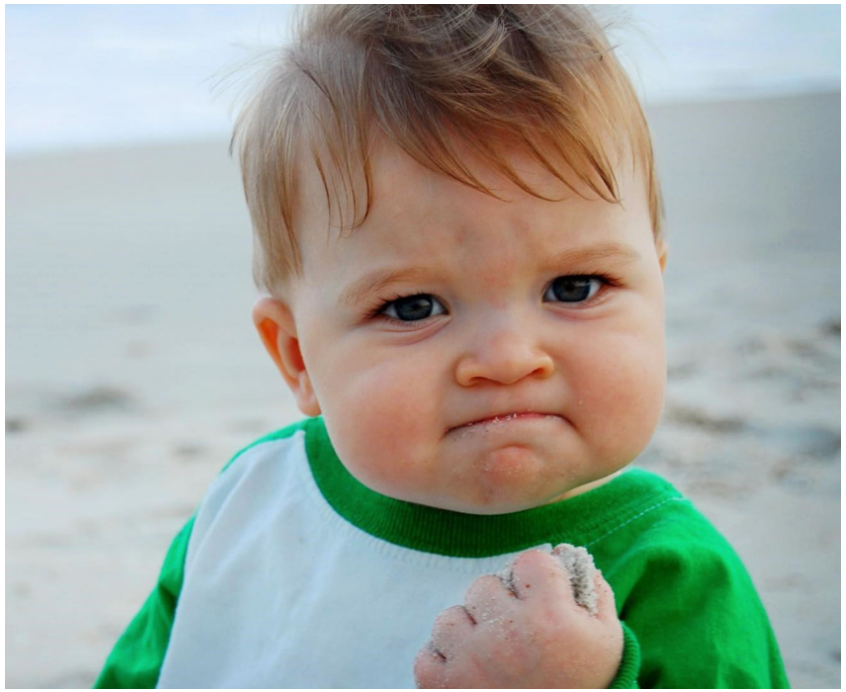
MICROSERVICES

IOT

EDGE

We can do this...

- Known good source / Source of truth
- Known good path
- CVE Scanning
- Repeatable and automated
- Chain of Custody (Audit Trail)



Source of Truth!

Code

Images

Two Good Starting Points

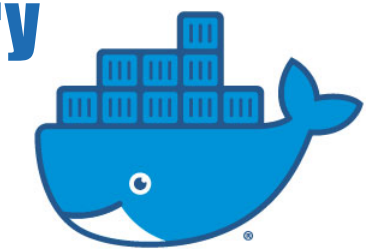
Fundamental Path

git commit

build number

Docker push

Docker Trusted Registry



tag

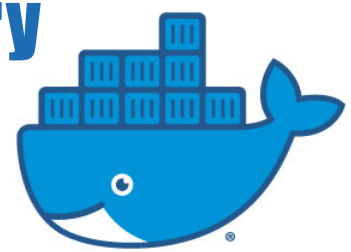
Image Signing

Webhook

Docker push

Notary

Docker Trusted Registry



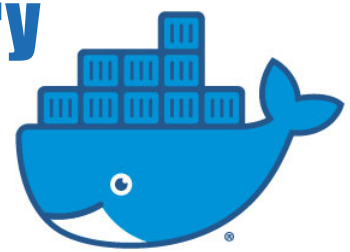
DTR Tooling

- CVE Scanning
- Promotion Policy (Internally)
- Mirroring Policy (Externally)
- Pruning Policy - Age Off
- RBAC - Control
- *Soon* - Full PKI Support

Quarantine?

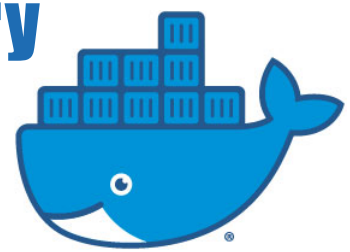
Quarantine

Docker Trusted Registry



Non-Prod

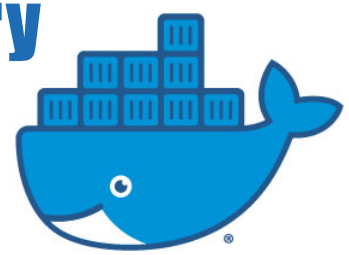
Docker Trusted Registry



Multiple Domains

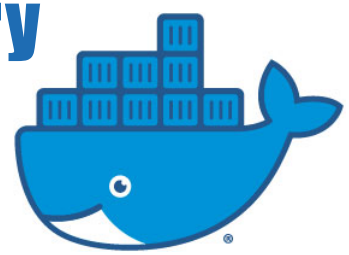
UnClassified

Docker Trusted Registry



Top Secret

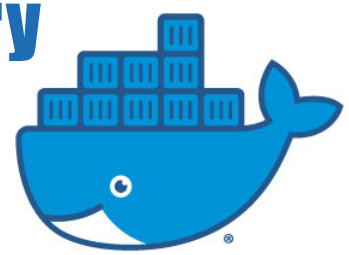
Docker Trusted Registry



Spoke and Hub?

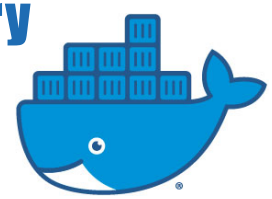
Non-Prod

Docker Trusted Registry



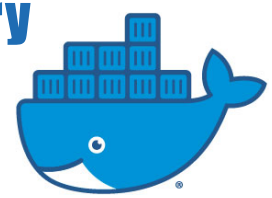
Prod - Cloud

Docker Trusted Registry

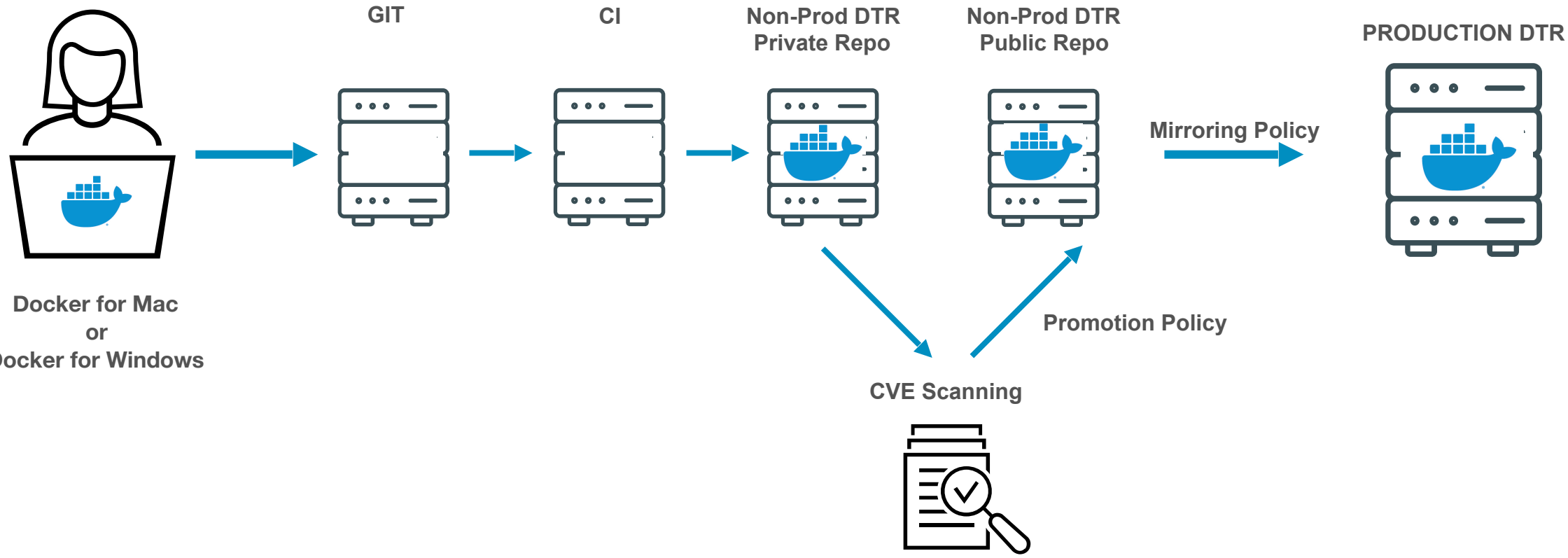


Prod - OnPrem

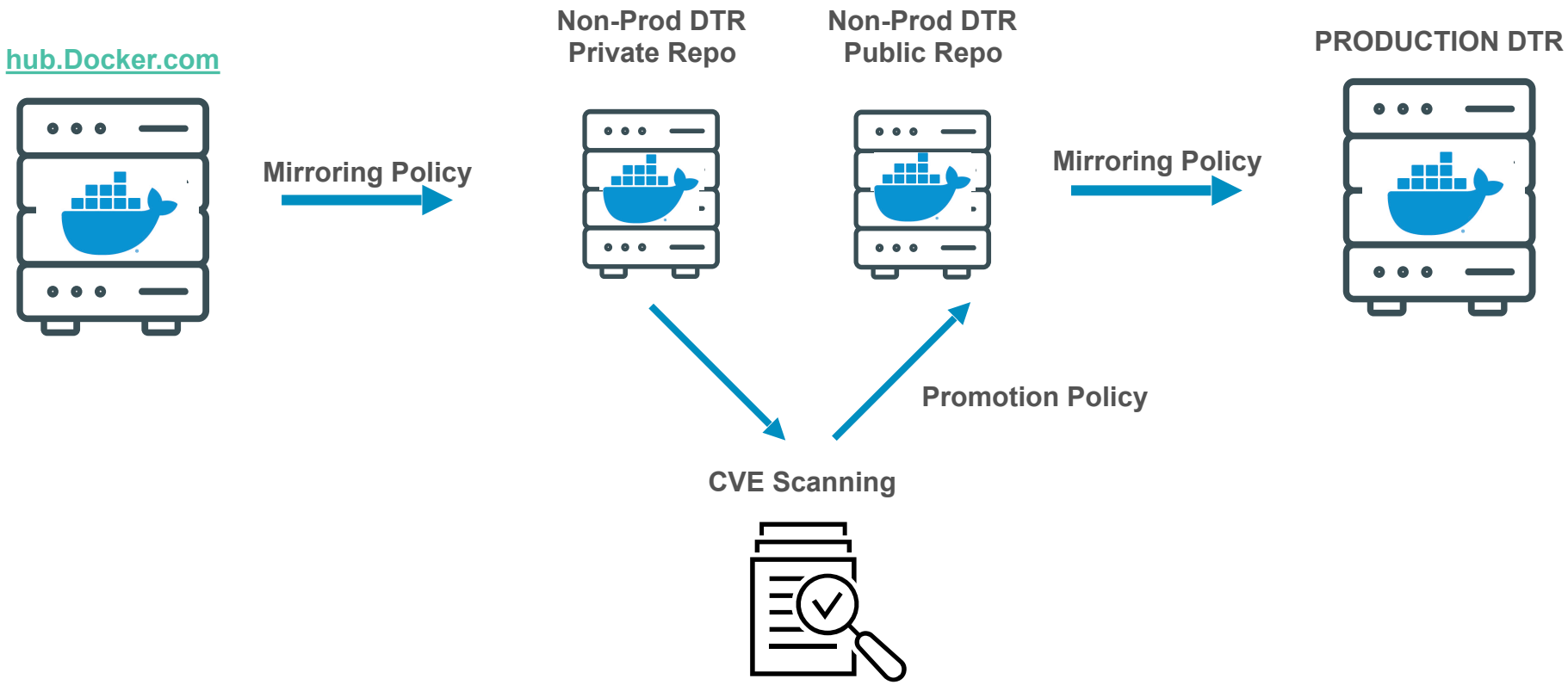
Docker Trusted Registry



Secure Supply Chain - Git Start

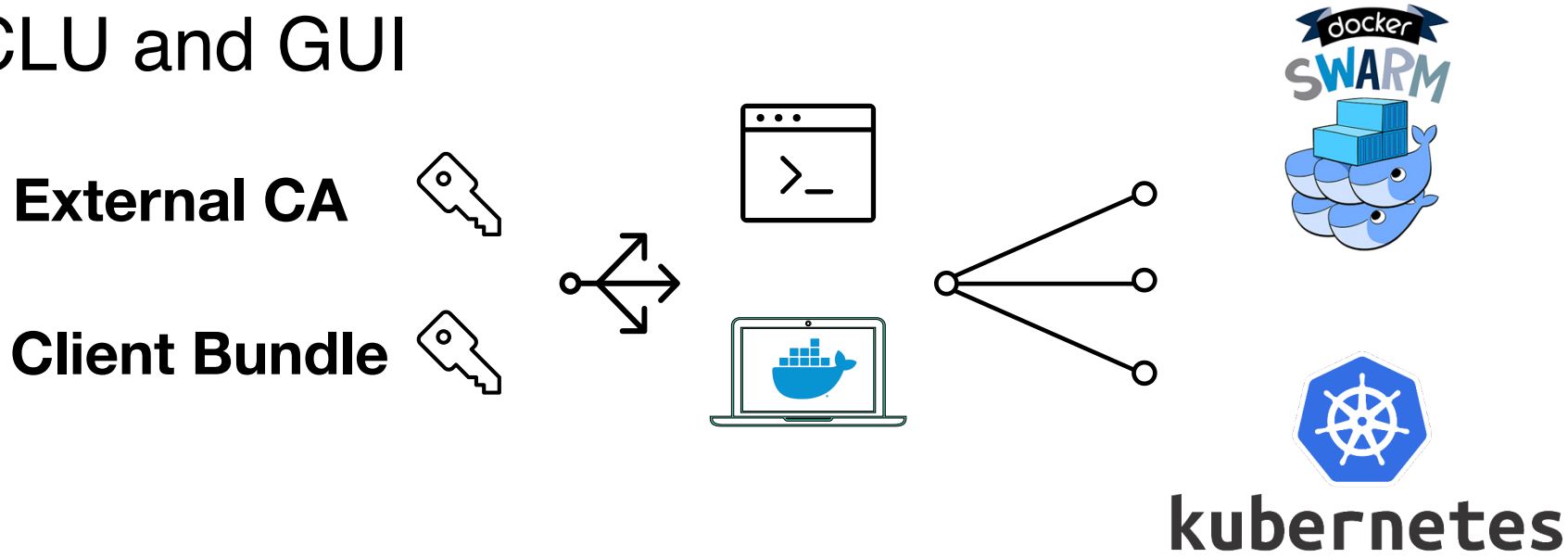


Secure Supply Chain - Docker Hub Start



Soon - PKI!

- No Passwords - Full Authentication
- Client Bundle or External CA
- UCP/DTR Swarm/Kubernetes
- CLU and GUI



Do you have a Secure Supply Chain?

- Known good source - Source of truth?
- Known good path?
- CVE Scanned?
- Repeatable?
- Chain of Custody (Audit Trail)?

Play - With - Docker (PWD)


https://andyc.info/dc19
@clemenko