andy clemenko - @clemenko - Docker

BUILDING A SECURE SUPPLY CHAIN

Please:

- Ask Questions
- Help each other
- Have fun
- Learn
- There will be prize…

What is NOT a Secure Supply Chain?

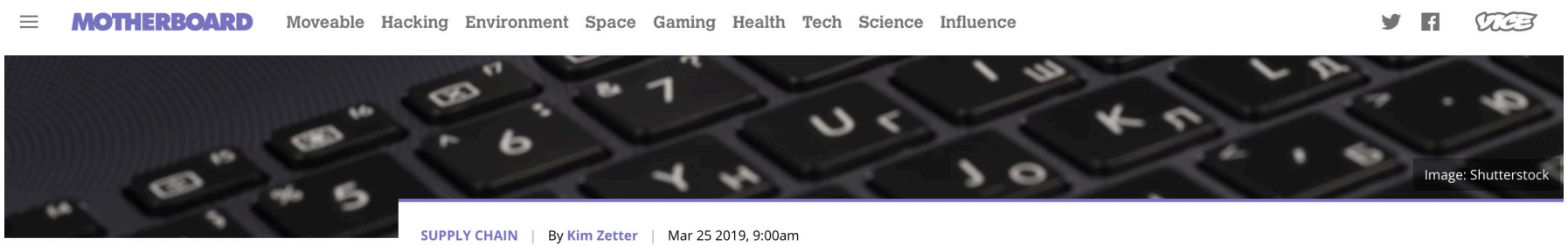
What is a Secure Supply Chain?

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

Why?

Honestly Why?

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

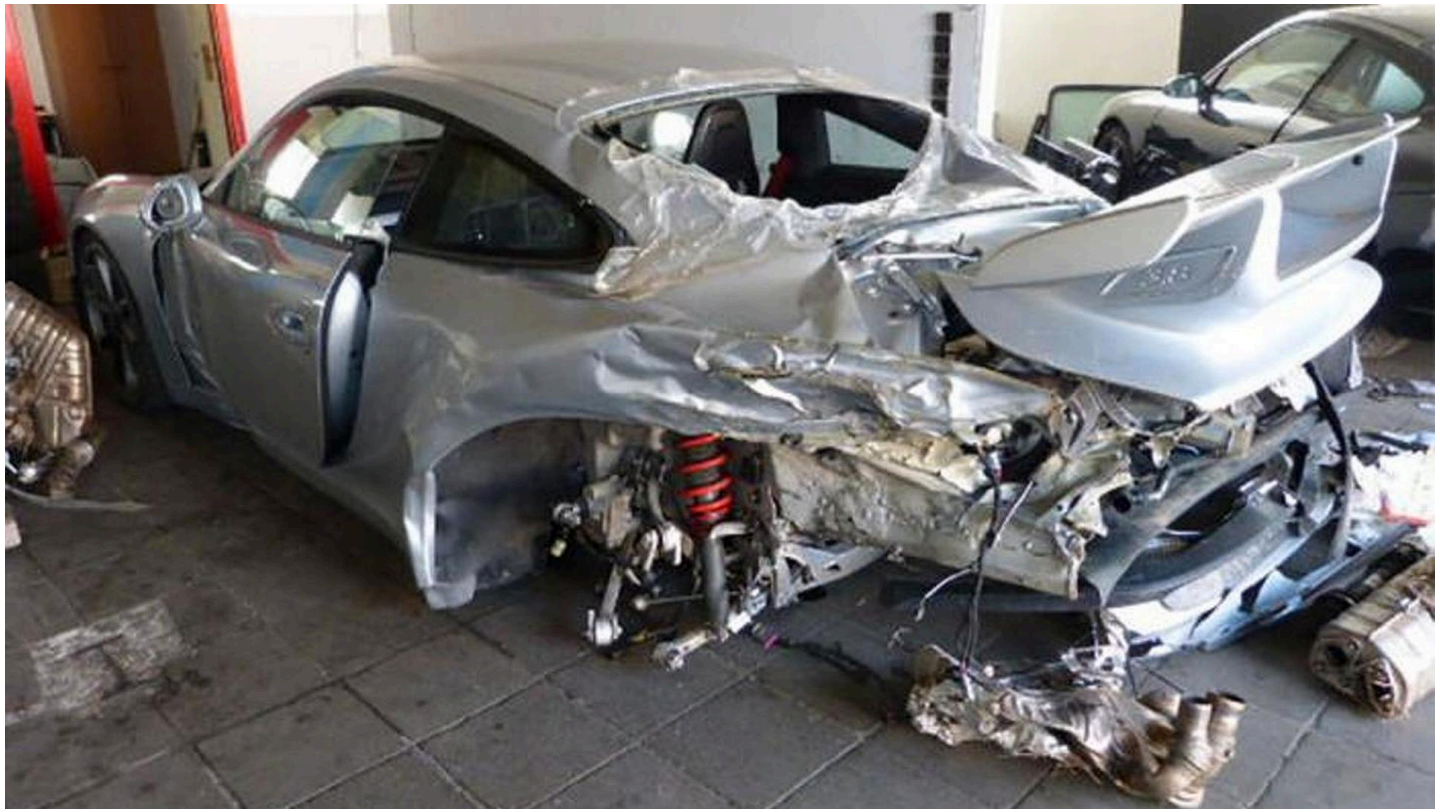
https://andyc.info/asus

Man in the Middle?

Docker pull from 35k feet!

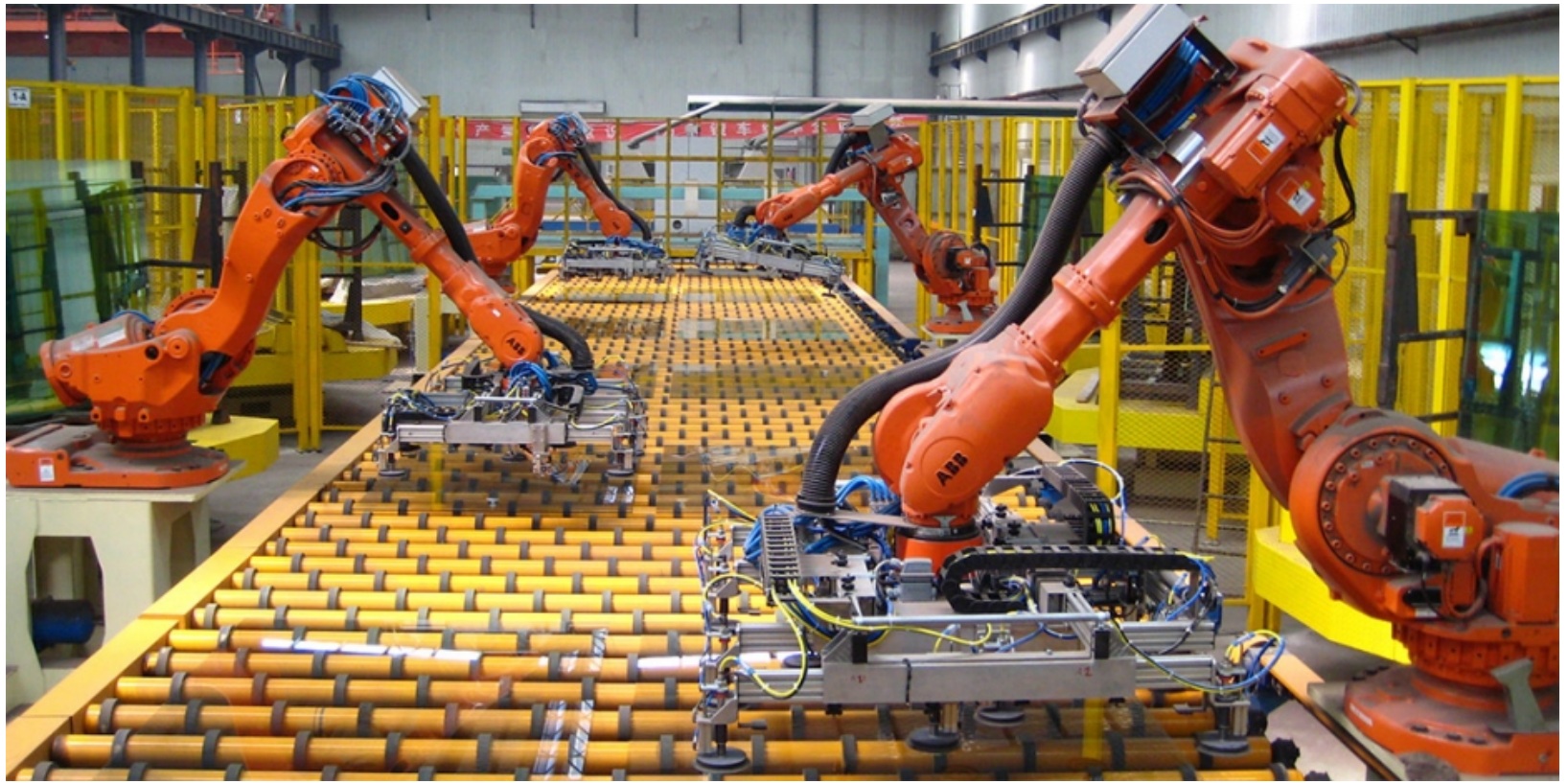
```
53116fdf277c: Download complete
ef355066beab: Download complete
b99ef0a573fc: Download complete
ed1862269ff7: Download complete
7e7cfef4f799: Downloading [==================>                ]  2.247MB/6.709MB
```

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

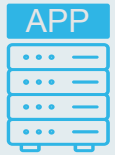
Scan out of date Retry

Chain of Custody?

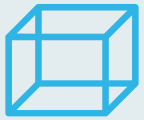
“No human should EVER build or deploy code meant for production!”

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

Images for everything!

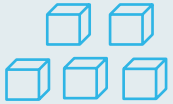


TRADITIONAL APPS



PACKAGED APPS

NEW APPS



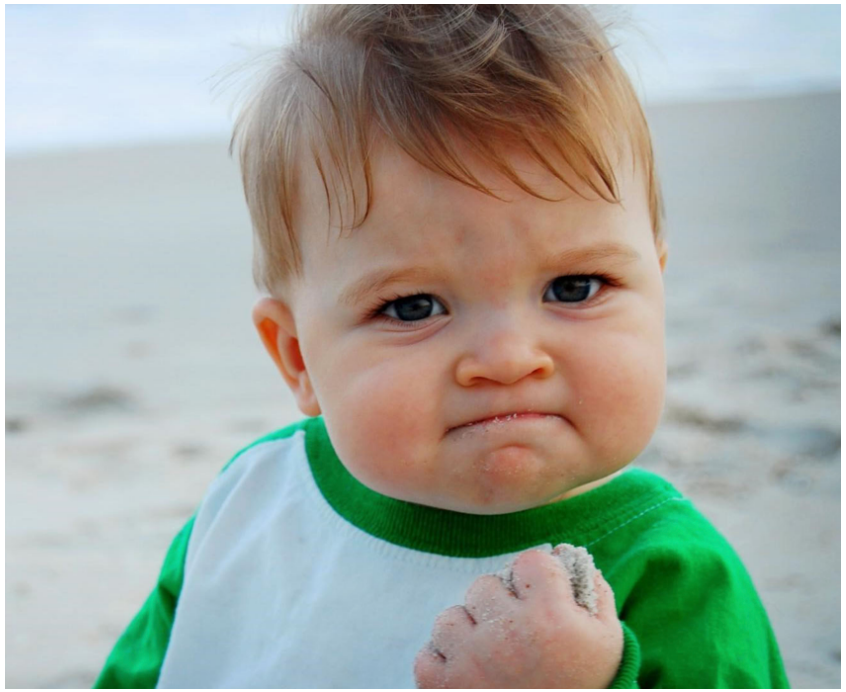
MICROSERVICES

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

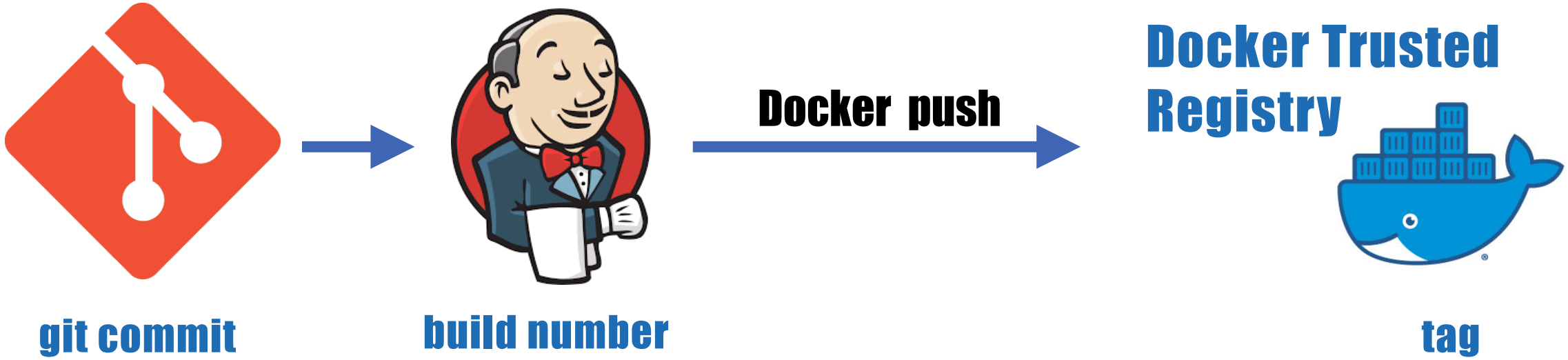


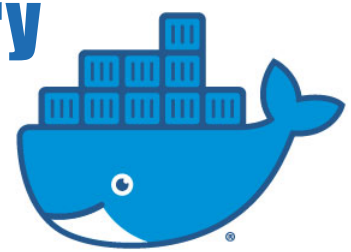
Image Signing

Webhook

Docker push

Notary

Docker Trusted Registry



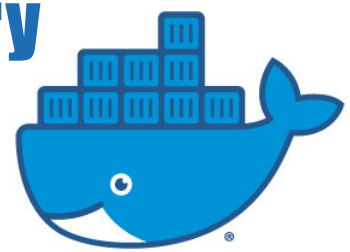
DTR Tooling

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

Quarantine?

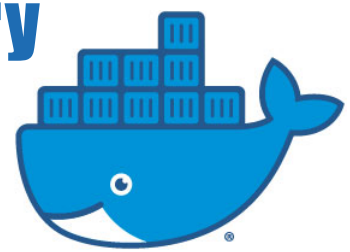
Quarantine

Docker Trusted Registry



Non-Prod

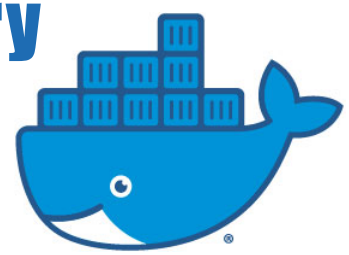
Docker Trusted Registry



Multiple Domains

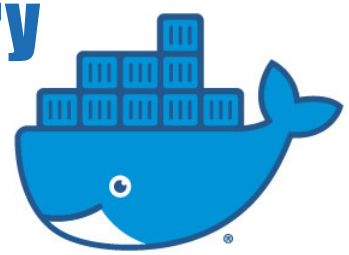
UnClassified

Docker Trusted Registry



Top Secret

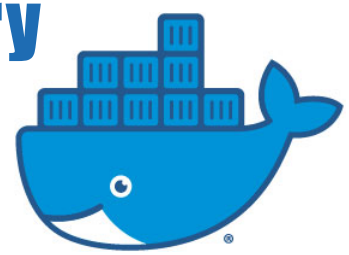
Docker Trusted Registry



Spoke and Hub?

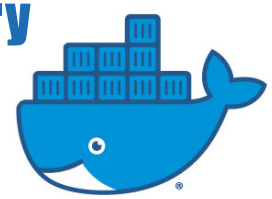
Non-Prod

Docker Trusted Registry



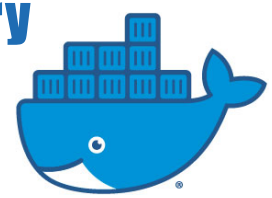
Prod - Cloud

Docker Trusted Registry

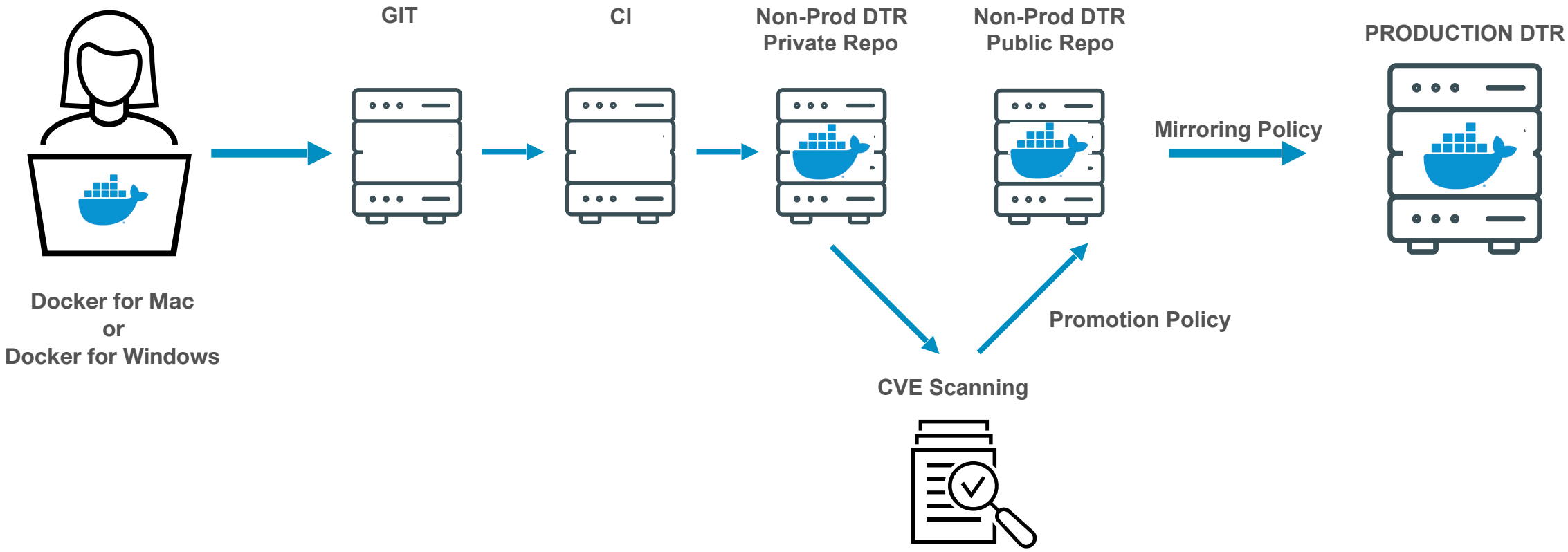


Prod - OnPrem

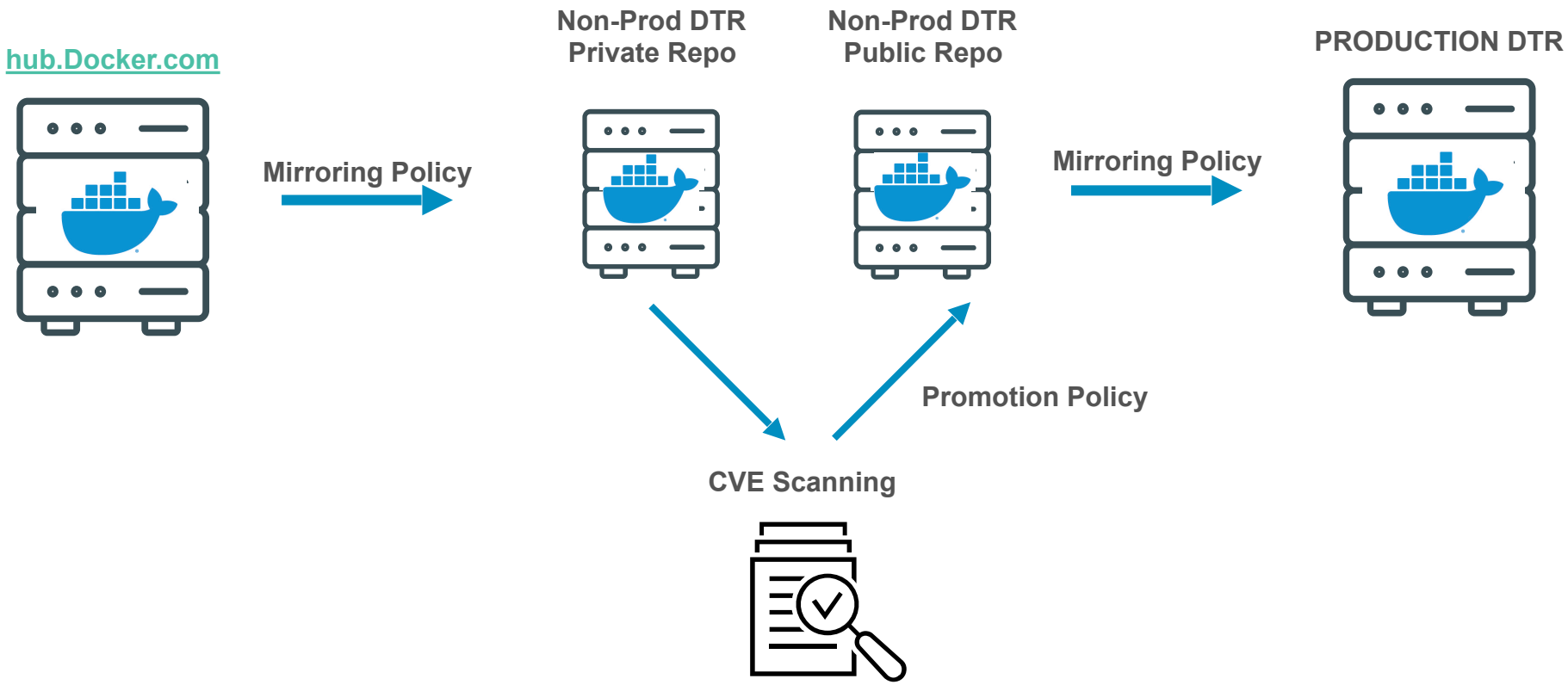
Docker Trusted Registry



Secure Supply Chain - Git Start

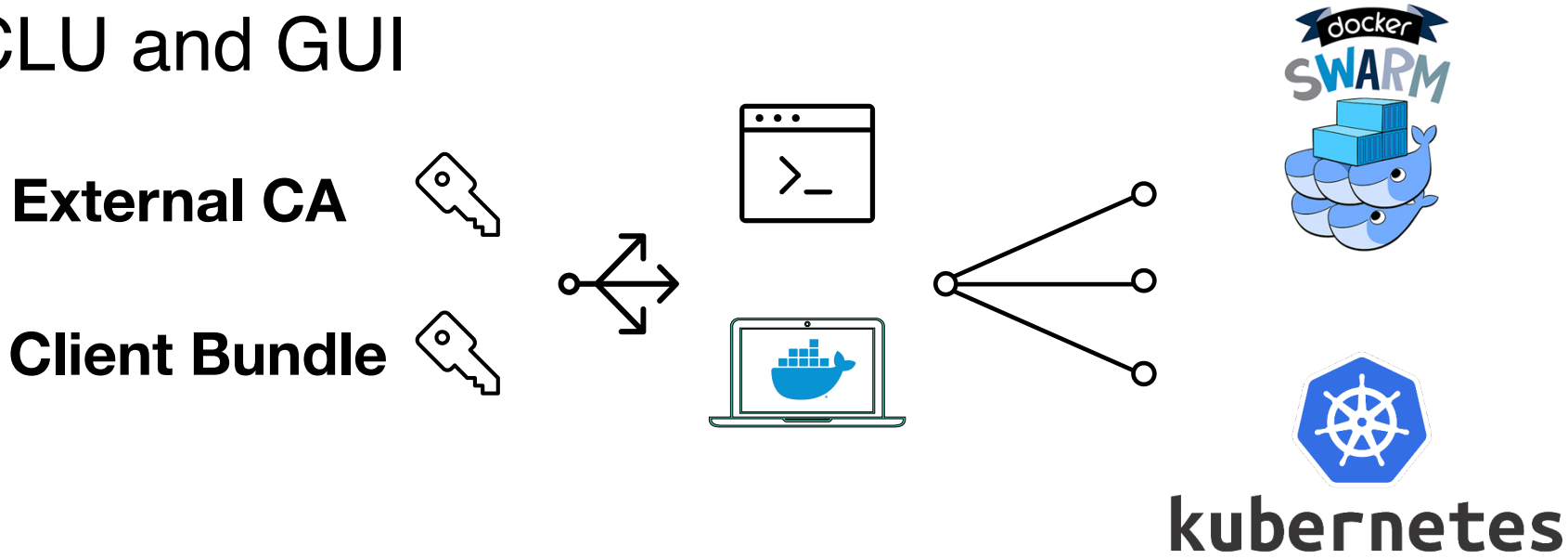


Secure Supply Chain - Docker Hub Start



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://dockr.ly/mid-atlsummit
https://andyc.info/summit19