



Building a Secure, Automated Supply Chain Workshop



<https://andy.c.info/dc19>

Please:

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

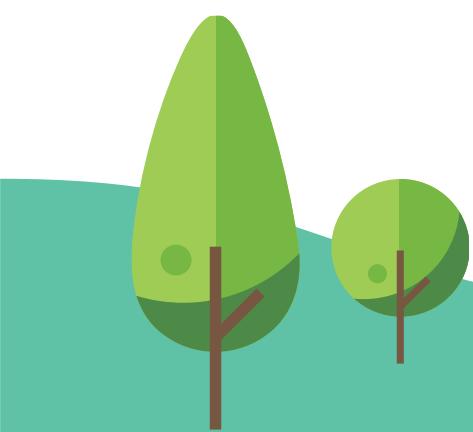
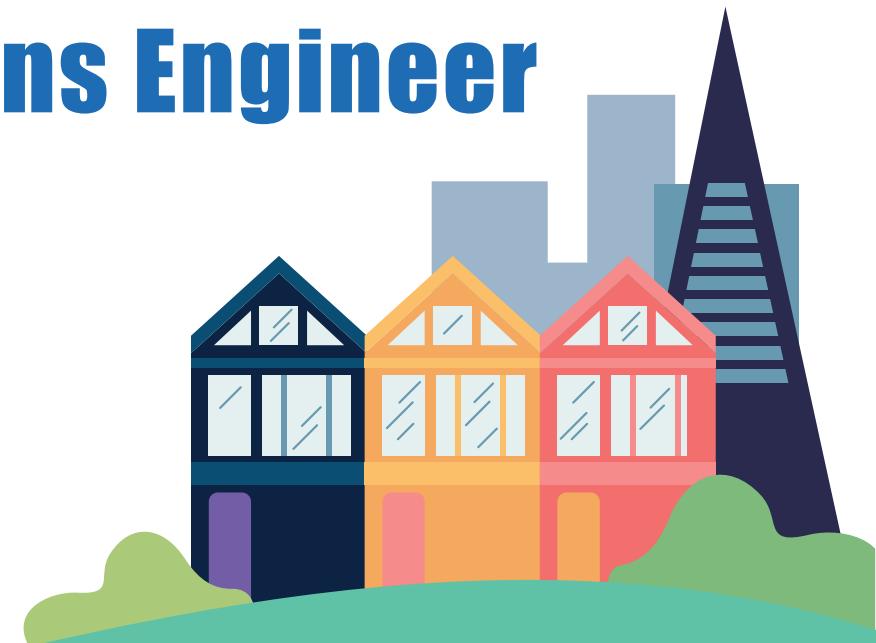


Andy Clemenko

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?

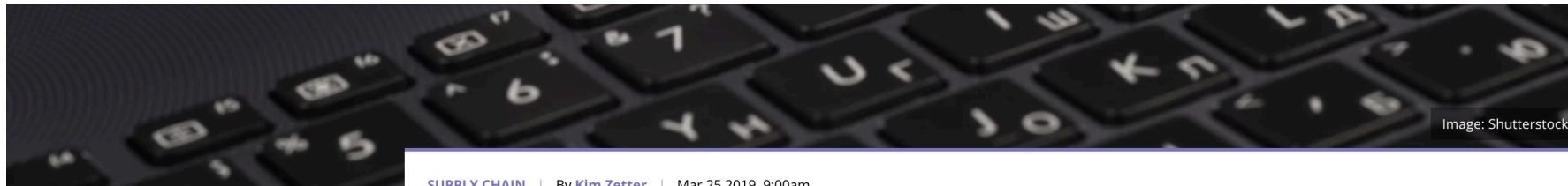
#dockercon19supplychainattack



Anyone have an Asus Laptop?

≡ MOTHERBOARD

Movable Hacking Environment Space Gaming Health Tech Science Influence



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
```

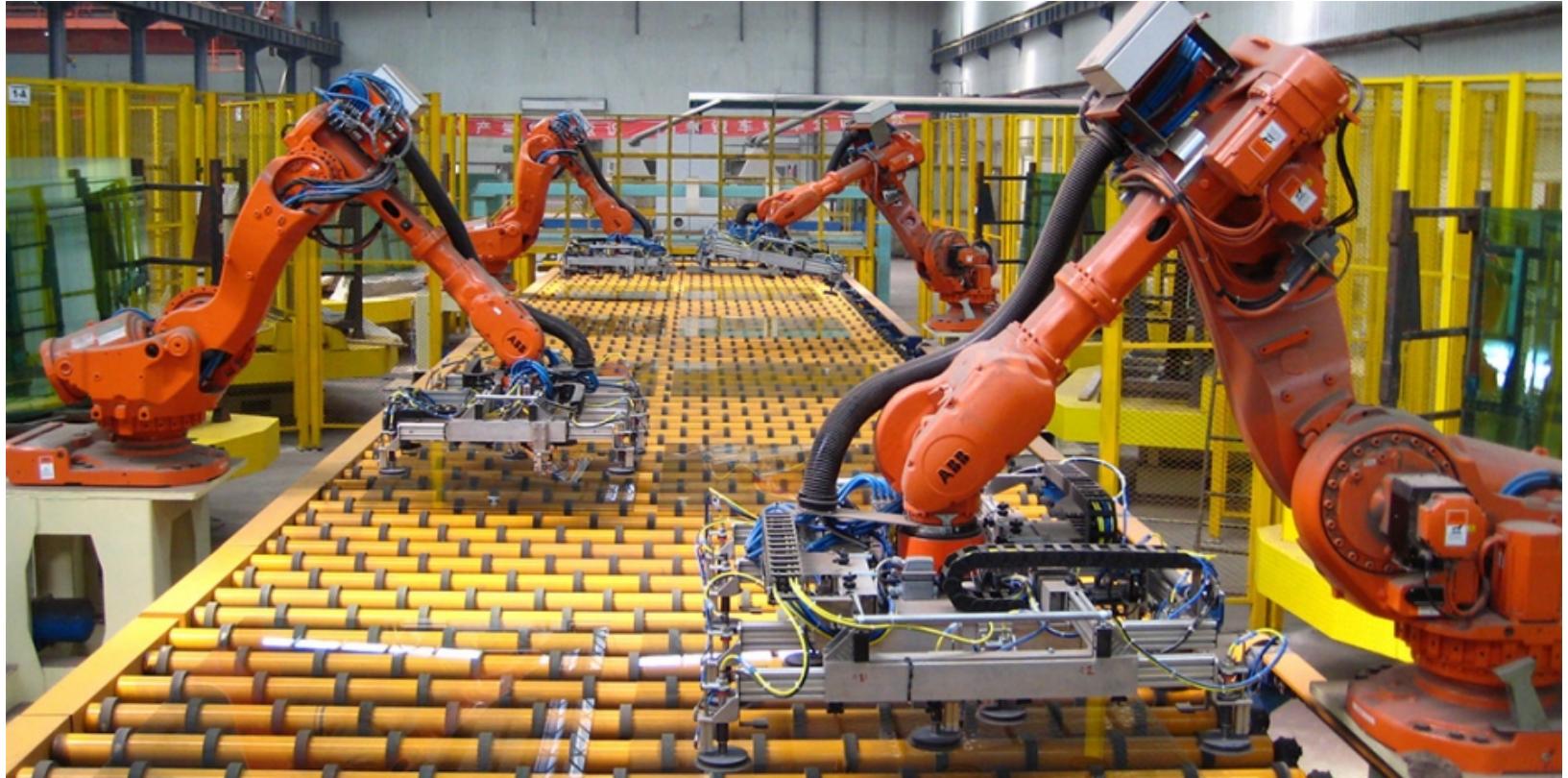
Replay Attack?



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 Scan out of date Retry ↻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?



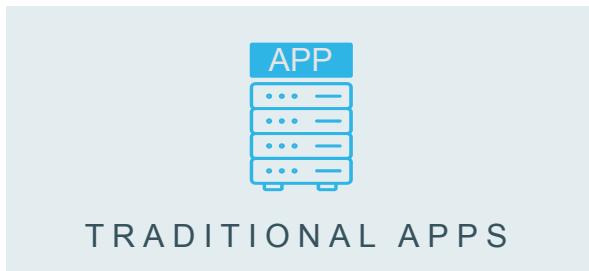
“No human should EVER build or deploy code meant for production!”



uvnik2009

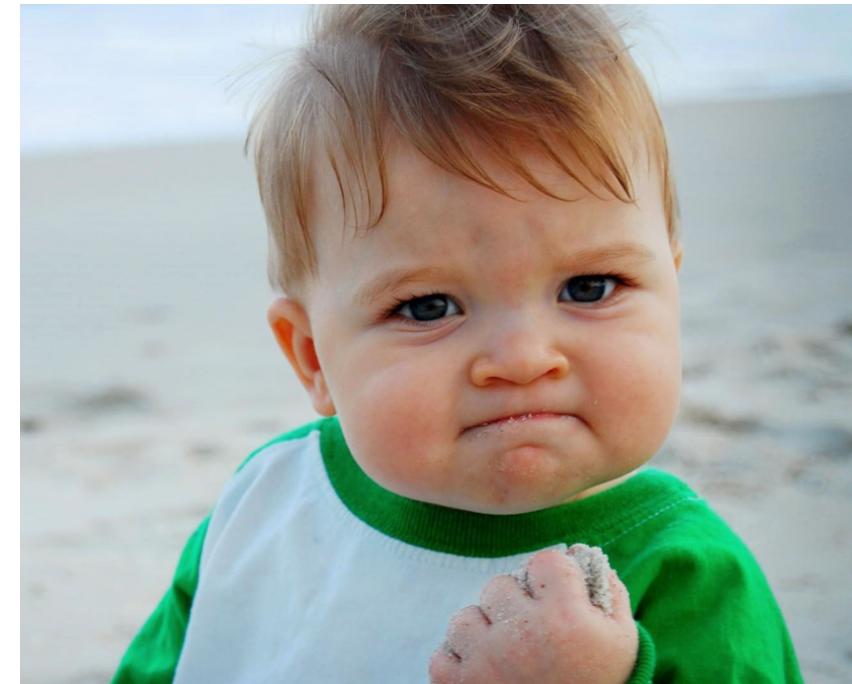
Image credit: <https://www.deviantart.com/uvnik/art/No-humans-allowed-142046016>

Images for everything!



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



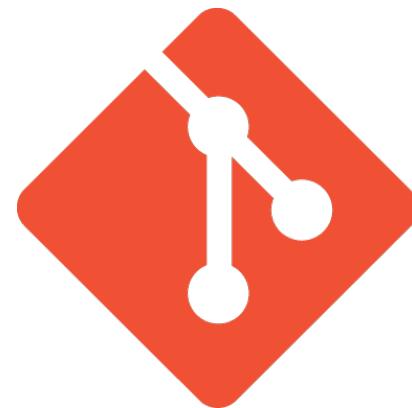
THERE CAN BE ONLY ONE

Images



THERE CAN BE ONLY ONE

Two Good Starting Points



Fundamental Path

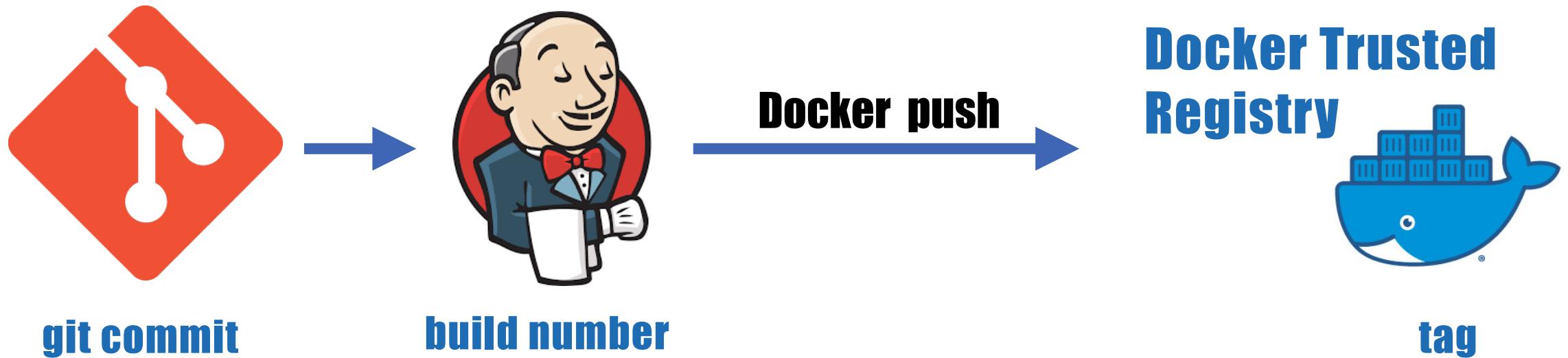
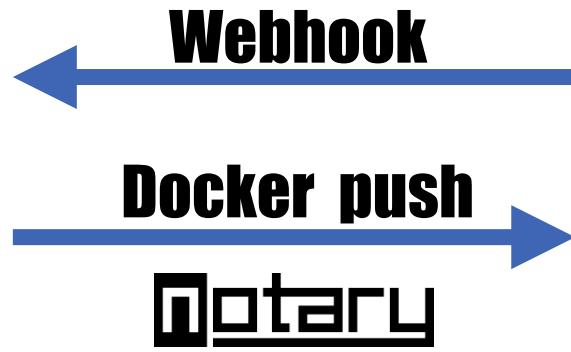
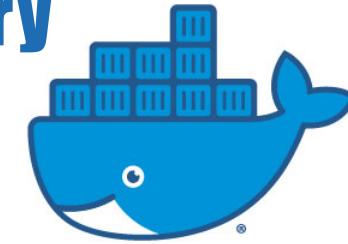


Image Signing



Docker Trusted
Registry

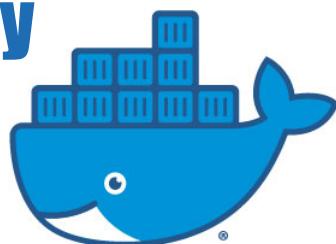


DTR Tooling

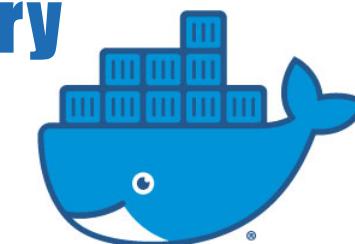
- CVE Scanning
- Promotion Policy (Internally)
- Mirroring Policy (Externally)
- Pruning Policy - Age Off
- RBAC - Control
- *Soon* - Full PKI Support

Quarantine?

Quarantine
Docker Trusted
Registry

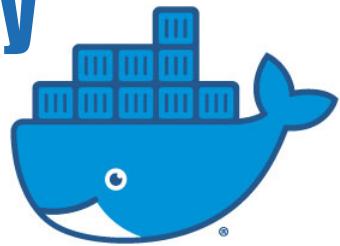


Non-Prod
Docker Trusted
Registry

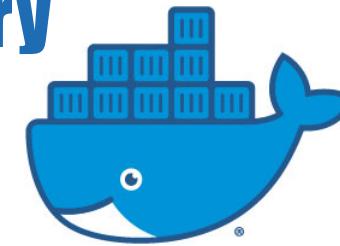


Multiple Domains

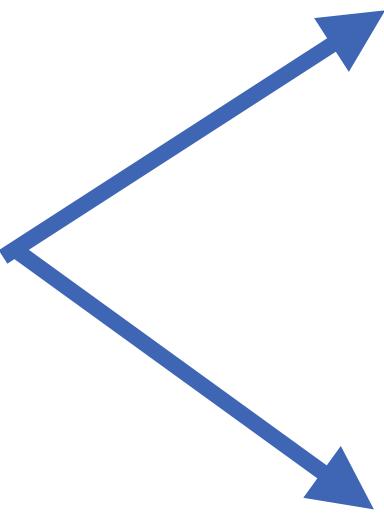
Unclassified
Docker Trusted
Registry



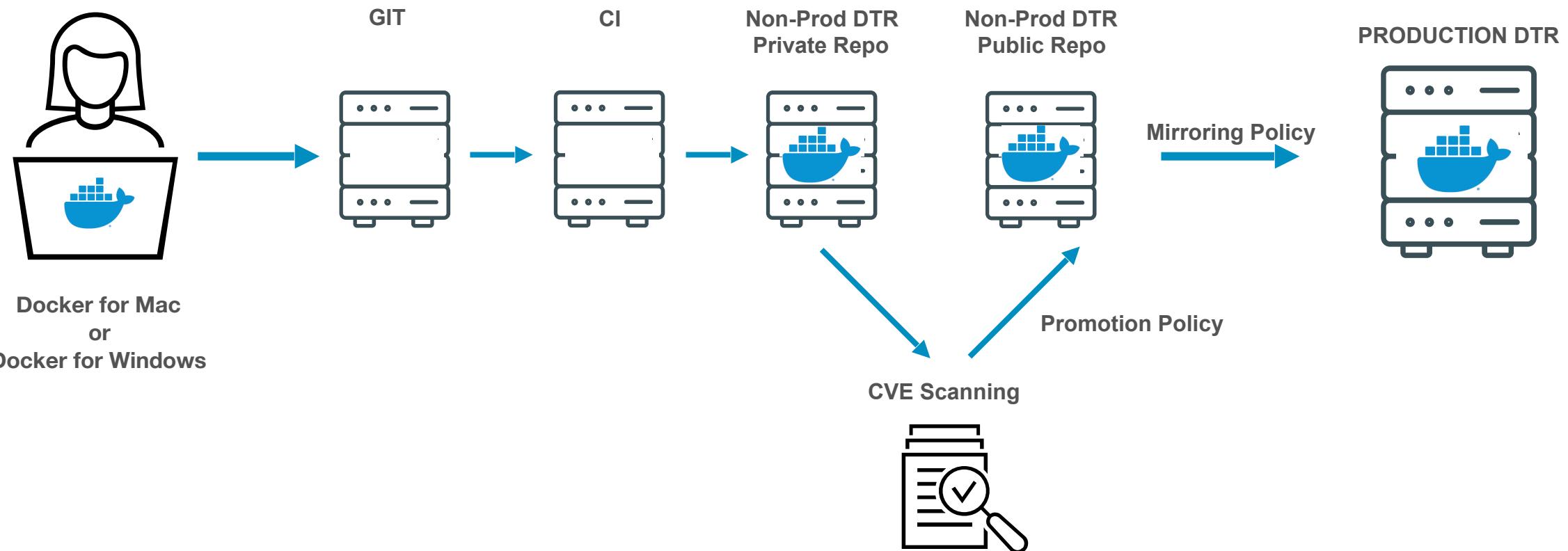
Top Secret
Docker Trusted
Registry



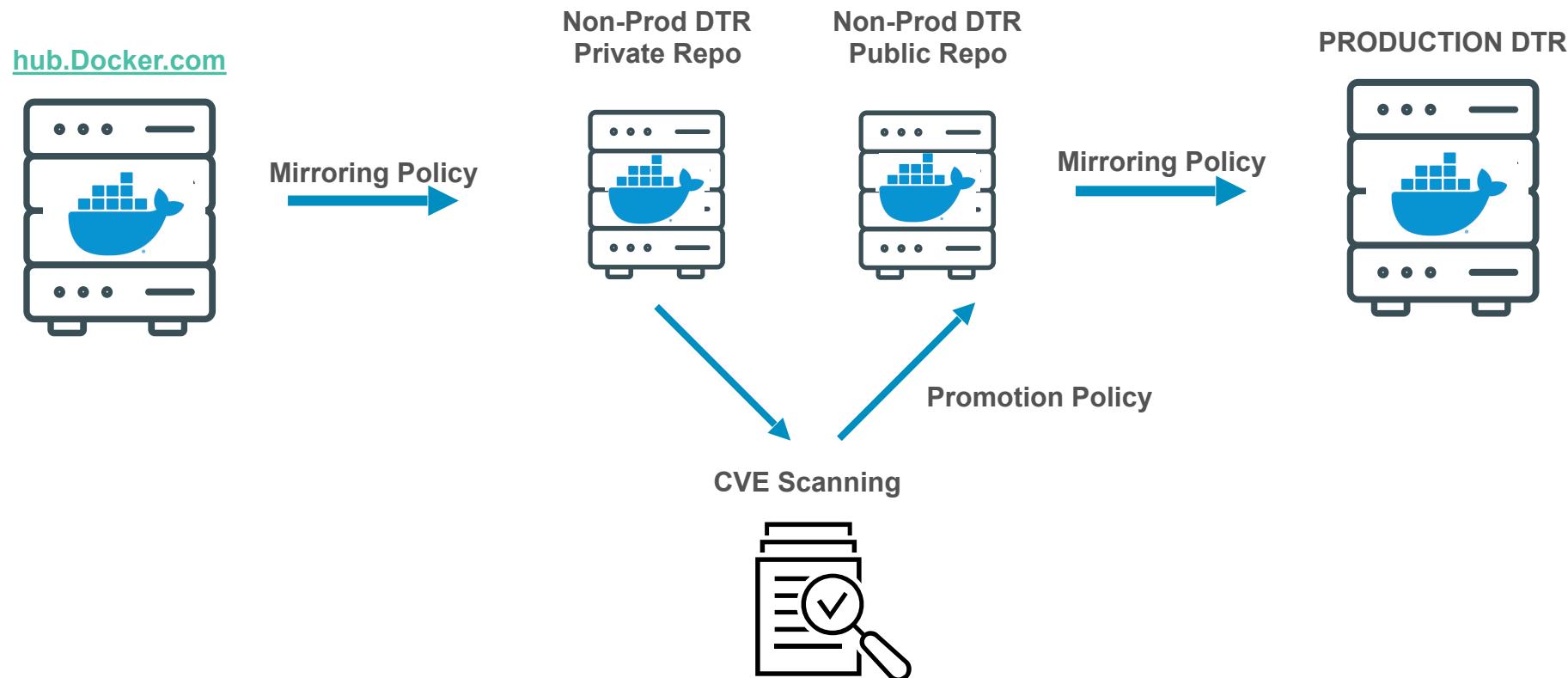
Spoke and Hub?



Secure Supply Chain - Git Start



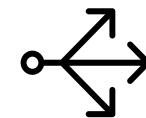
Secure Supply Chain - Docker Hub Start



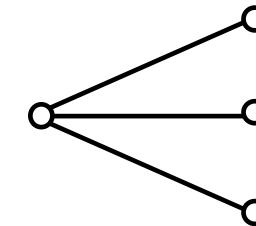
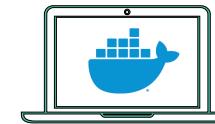
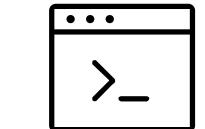
Soon - PKI!

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

External CA



Client Bundle



kubernetes

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)



A photograph of the Golden Gate Bridge in San Francisco, California, during sunset. The bridge's towers and cables are illuminated with a warm, orange-red glow against a backdrop of a clear blue sky transitioning into a soft orange and yellow near the horizon. The water of the San Francisco Bay reflects the colors of the sky. In the foreground, the tops of some low-lying, golden-brown bushes are visible.

[@clemenko](https://andy.c.info/dc19)