CLOUDNATIVE SECURITYCON

NORTH AMERICA 2023

CLOUDNATIVE
SECURITYCON
NORTH AMERICA 2023

Secure your Software Supply Chain at Scale

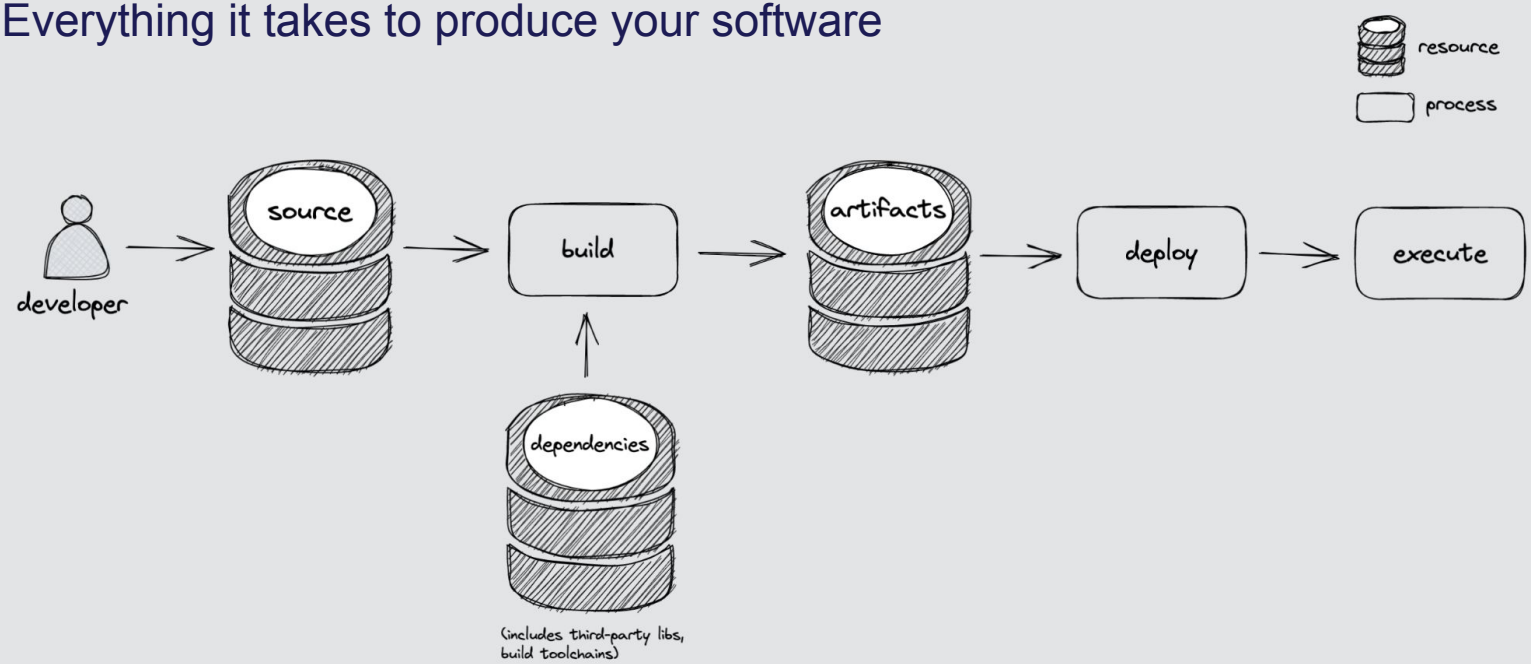
Hemil Kadakia & Yonghe Zhao, Yahoo

Agenda

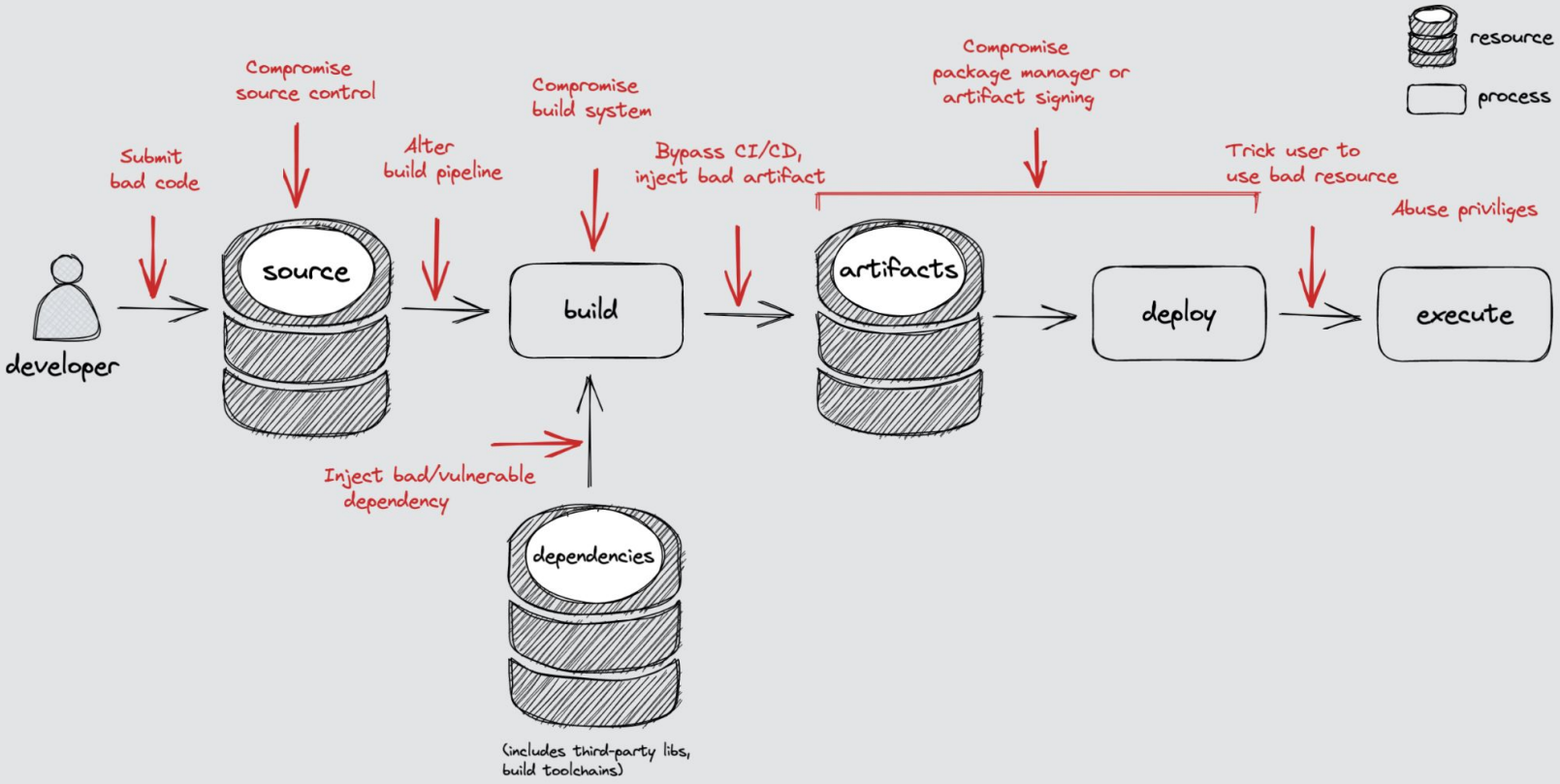
- What is software supply chain & why is it important?
- Existing solutions
- Infrastructure & Scale at Yahoo!
- Demos & deep dive
- Lessons learned

What is the software supply chain?

- Everything it takes to produce your software



What is the problem?



Why is it important to us?

Twilio Hackers Scarf 10K Okta Credentials in Sprawling Supply Chain Attack

DEVELOPER BEWARE —

Backdoor in public repository used new form of attack to target big firms

Dependency confusion attacks exploit our trust in public code repositories.

Attacker Breach 'Dozens' of GitHub Repos Using Stolen OAuth Tokens

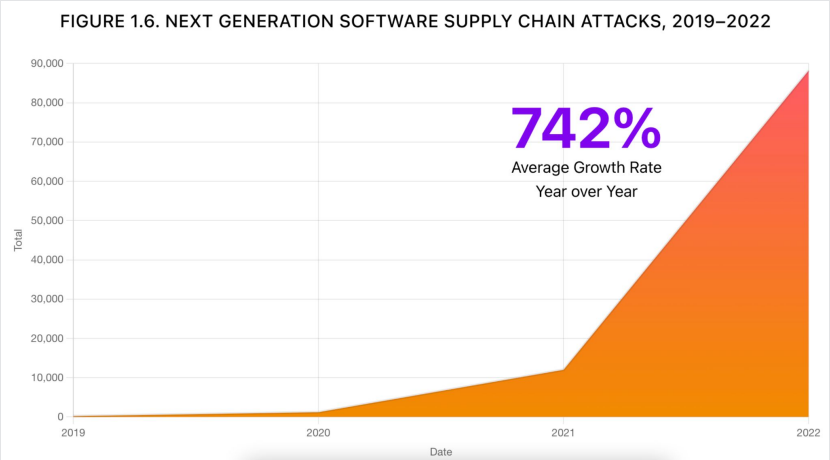
Magento Supply Chain Attack Targets Extension Developer FishPig

PyTorch suffers supply chain attack via dependency confusion

A rogue packet on the machine learning framework allowed the attacker to exfiltrate data, including SSH keys.

Recent studies

- 85 to 97% of enterprise codebase uses open source software
- Three out of Five Companies Targeted - Anchore
- 62% of Organizations Have Been Impacted by Software Supply Chain Attacks - Anchore



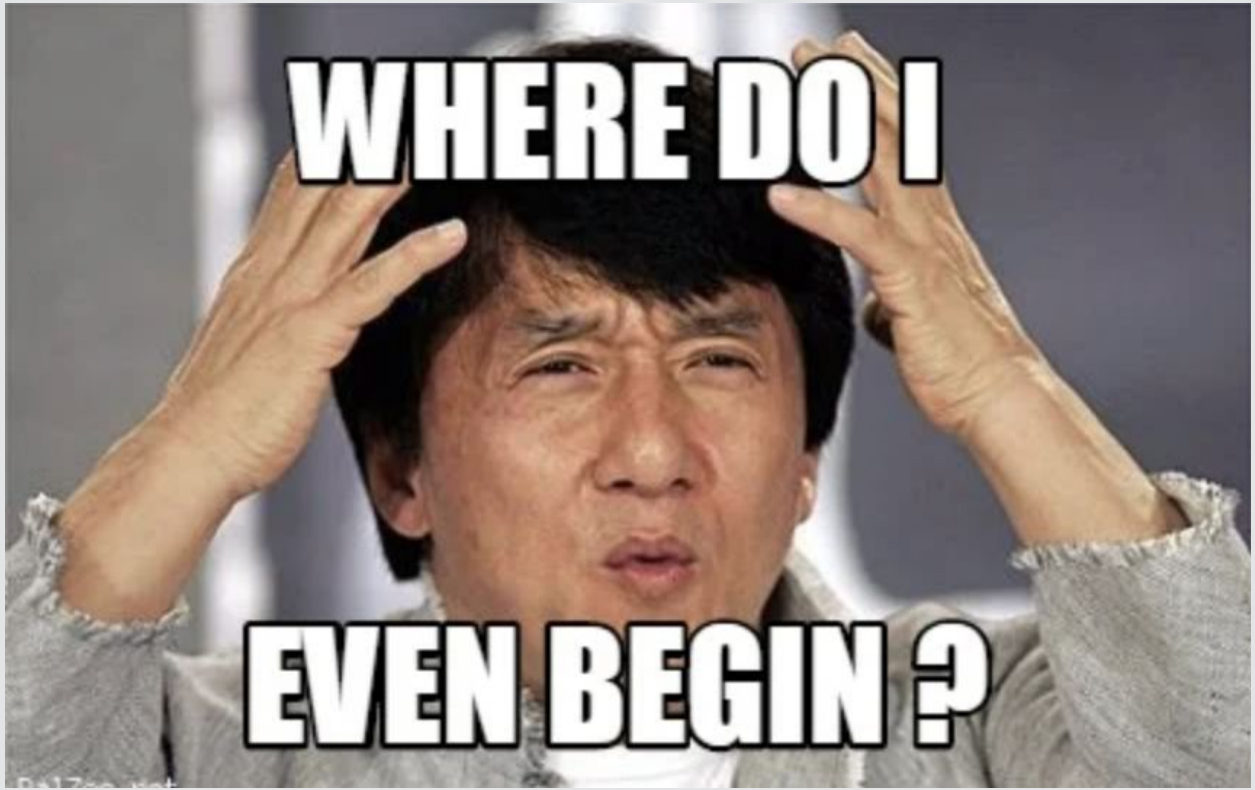
[Anchore's software supply chain security report]
[Sonatype's state of the software supply chain]

Existing standards/tools.

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

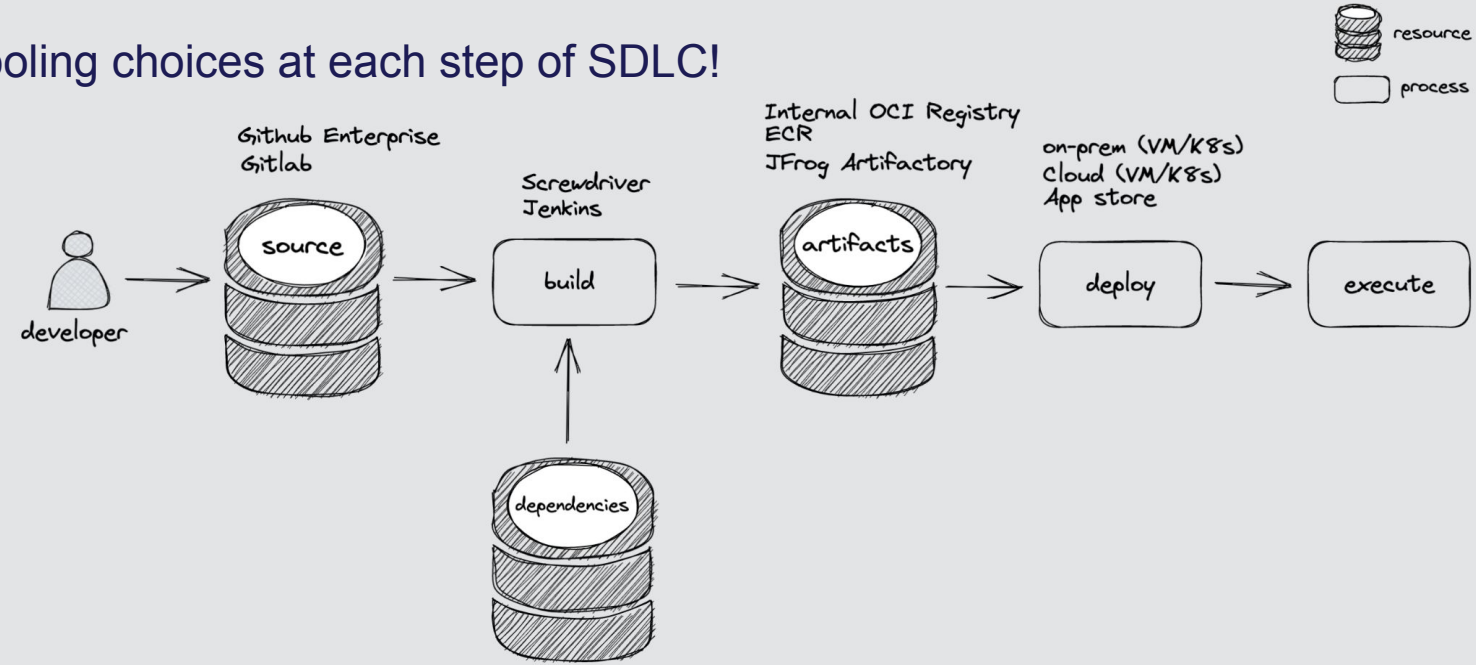
Additional reading: TAG Security Resources

But…

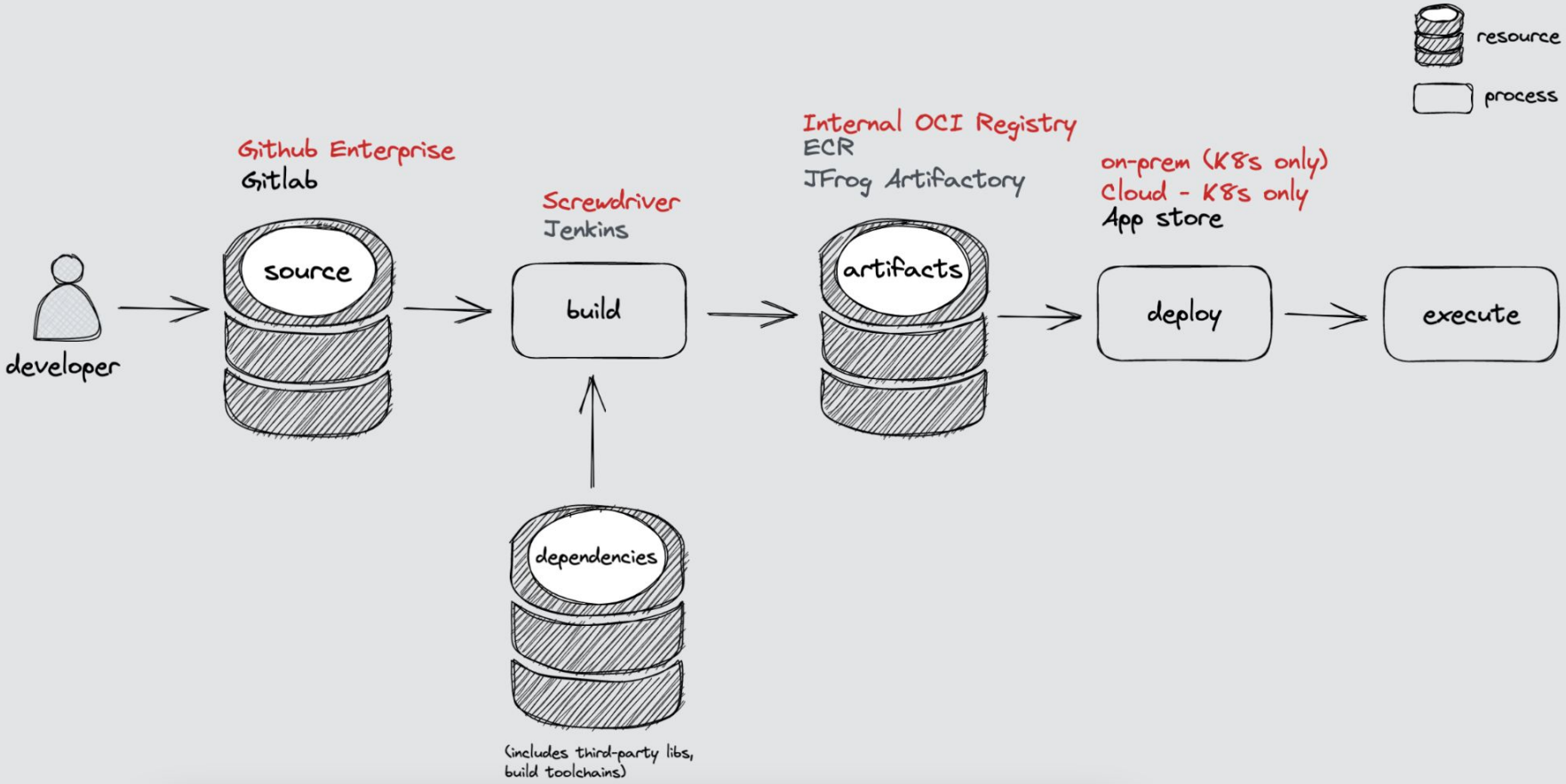


Current State at Yahoo!

- 60k daily builds and 5k images published per day.
- 700+ K8s clusters and 100k+ pods running.
- Many tooling choices at each step of SDLC!



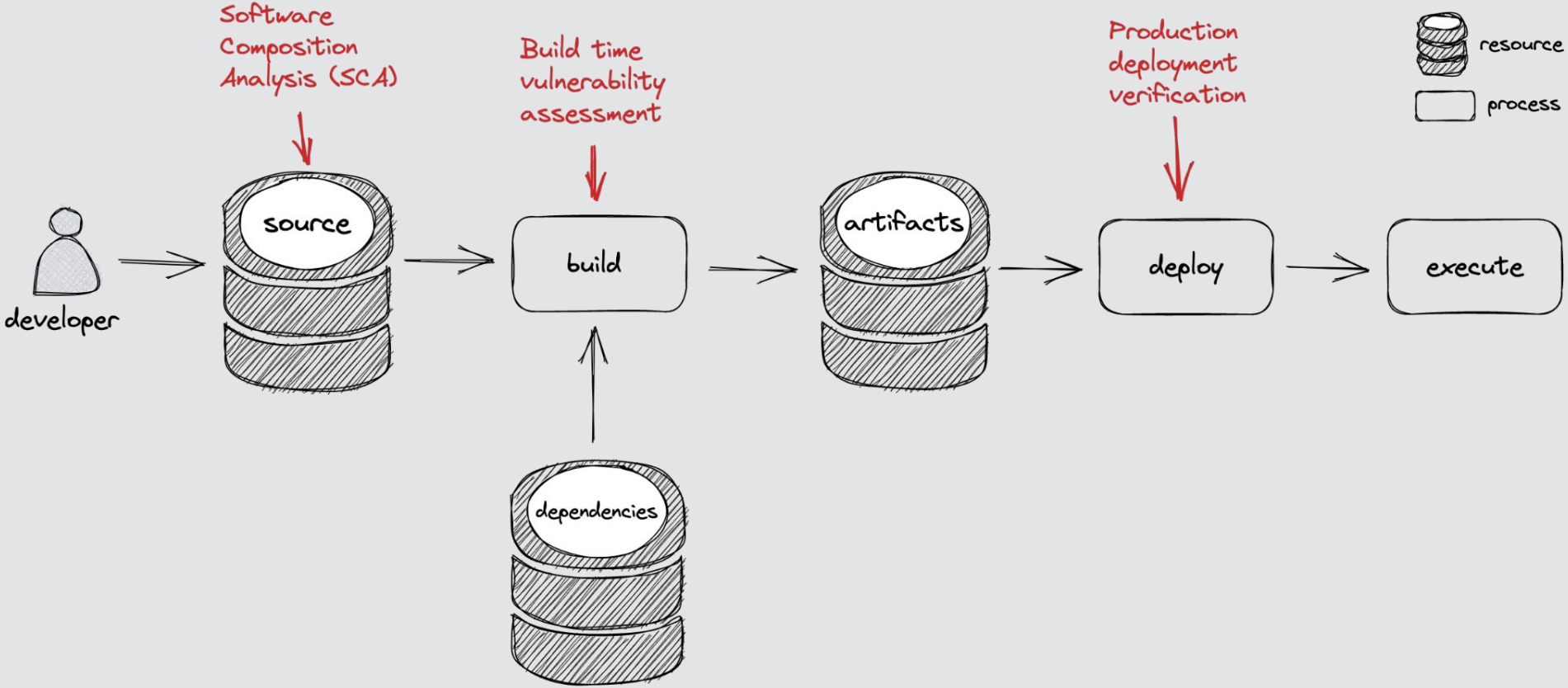
Choose your battles wisely



Existing security controls

- Static code scanning.
- GitHub branch protection & 2 PR reviewers.
- MFA & SSH keys for GitHub operations.
- Ephemeral creds in build environment.
- Mirror external registry.
- …

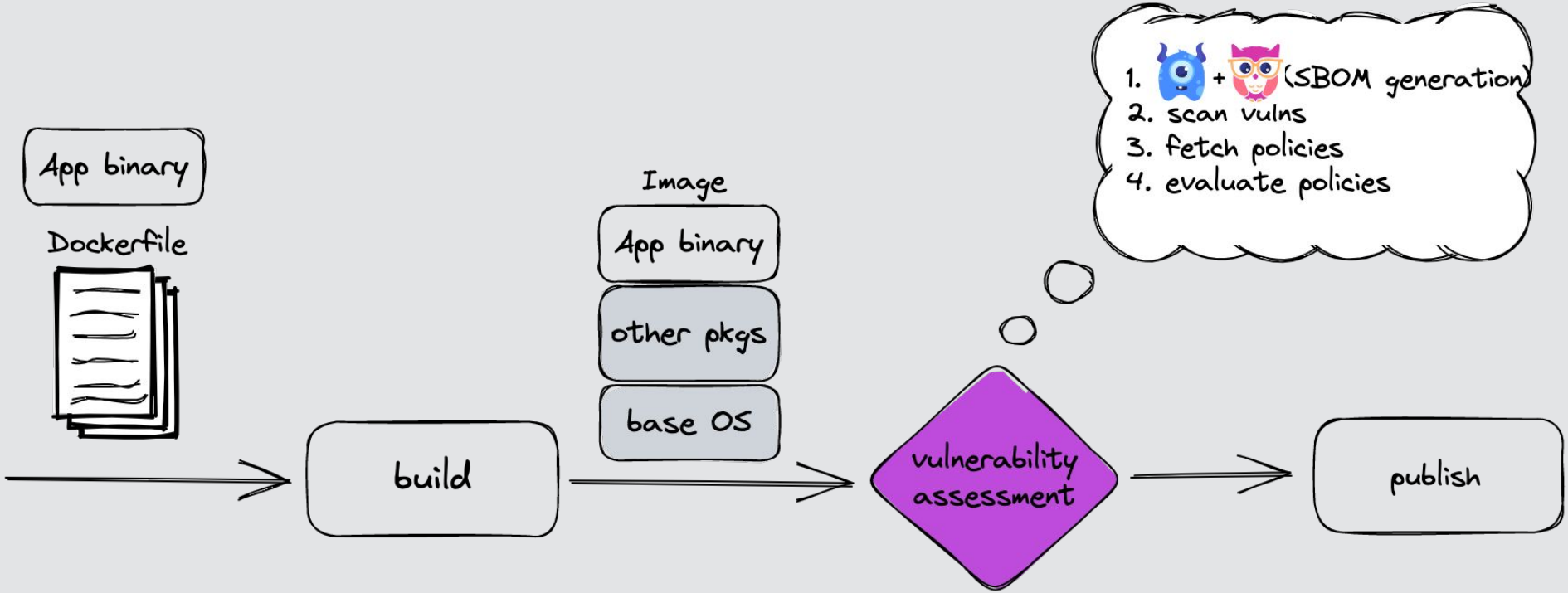
Starting our journey



Software Composition Analysis (SCA)

- SCA checks only vulnerabilities in open source dependencies.
- 97% of open source vulnerabilities can be fixed by updating to the latest version.
- Auto remediation of security vulnerabilities.

Build time vuln assessment



Production deployment verification

- Image provenance check.
- Image signature check.
- Image freshness check.
- …

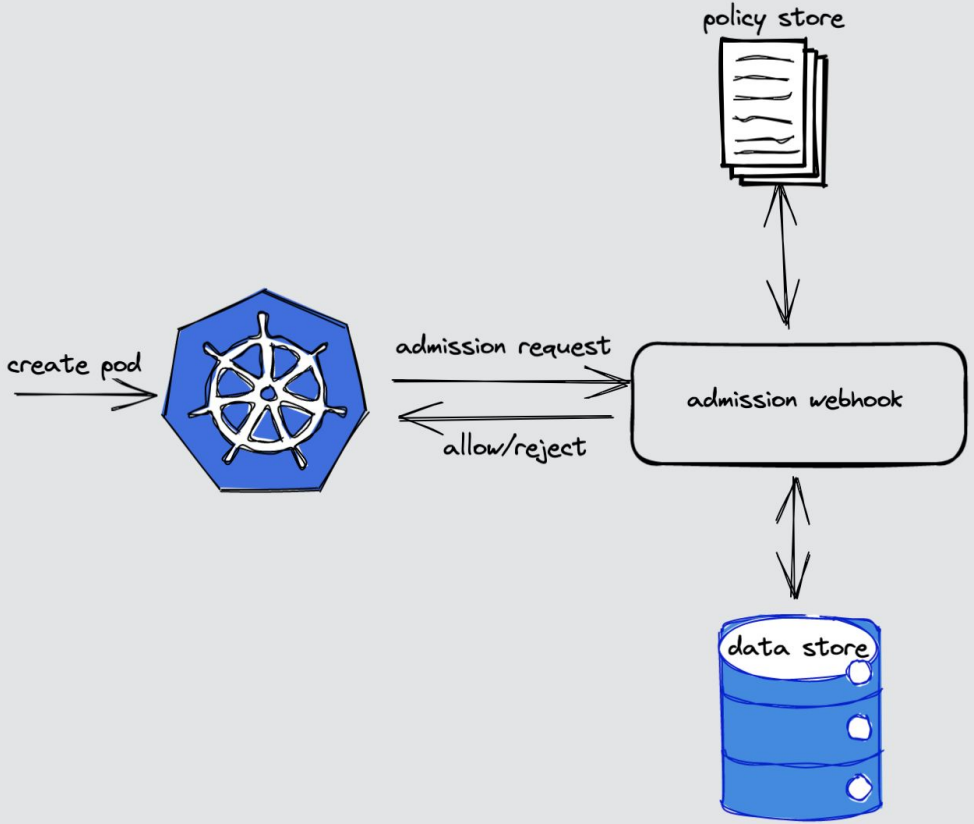


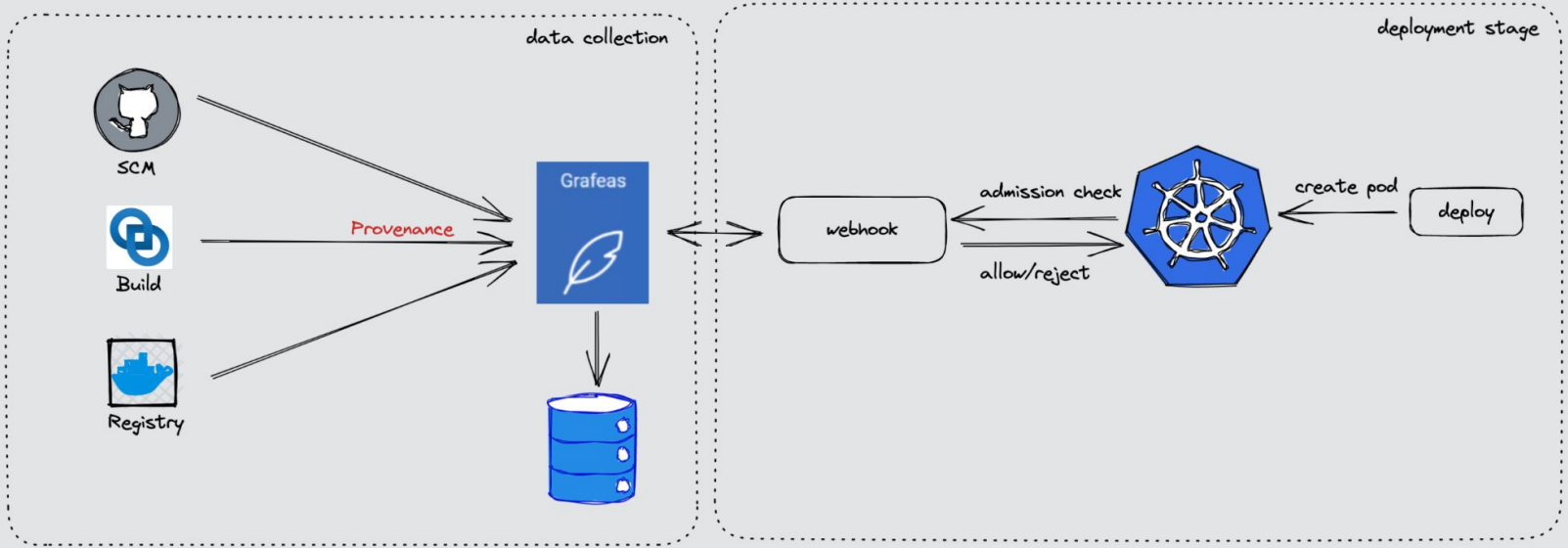
Image provenance check

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

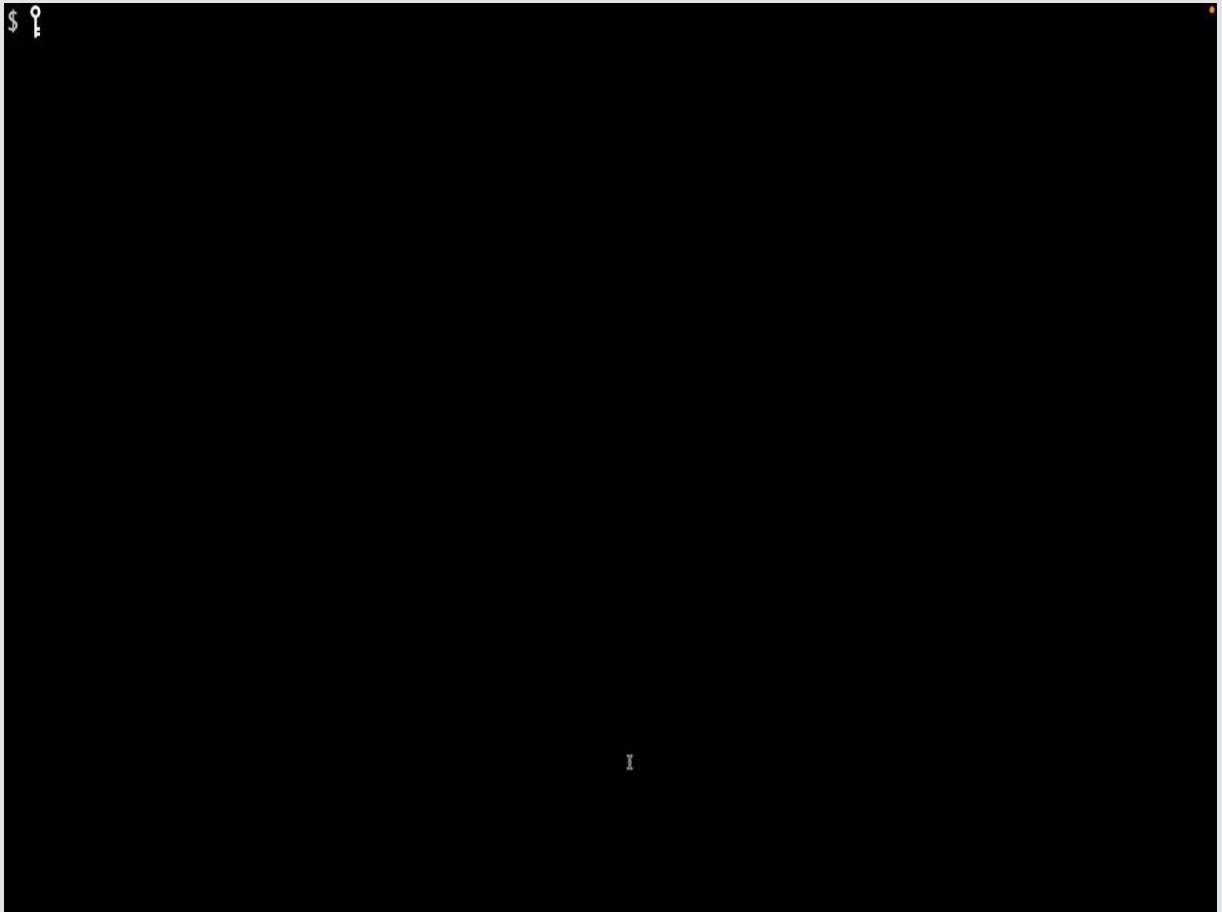
Provenance: records that tell you where this image comes from.

Provenance helps us to ensure images are:

- built from only allowed repo/branch/tag
- built using supported CI/CD pipelines
- …



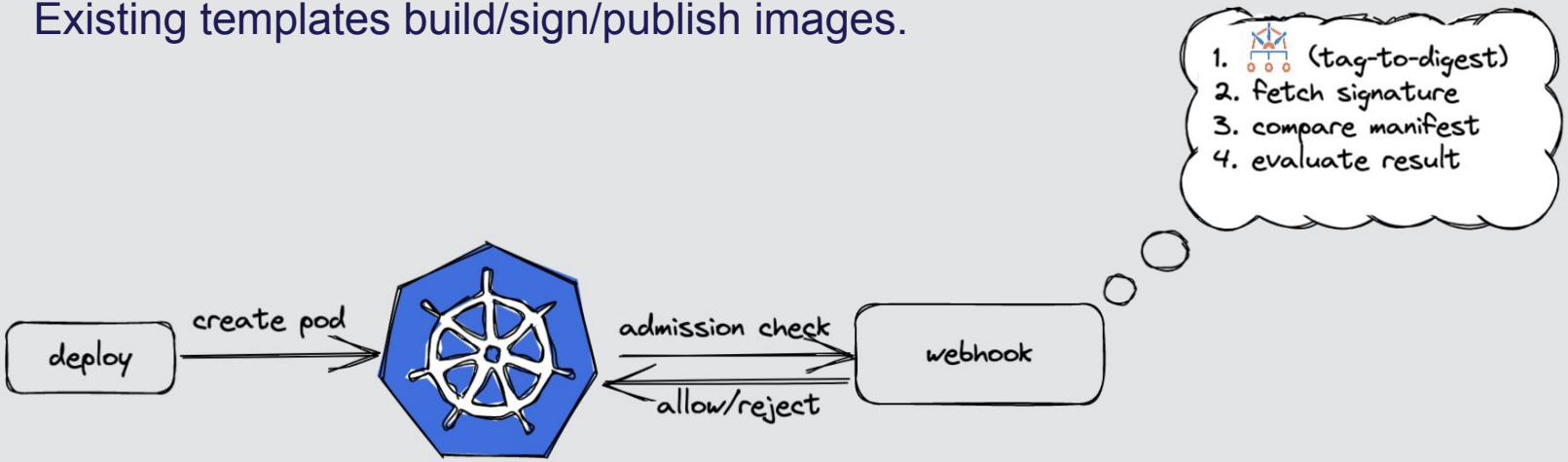
Demo: provenance check



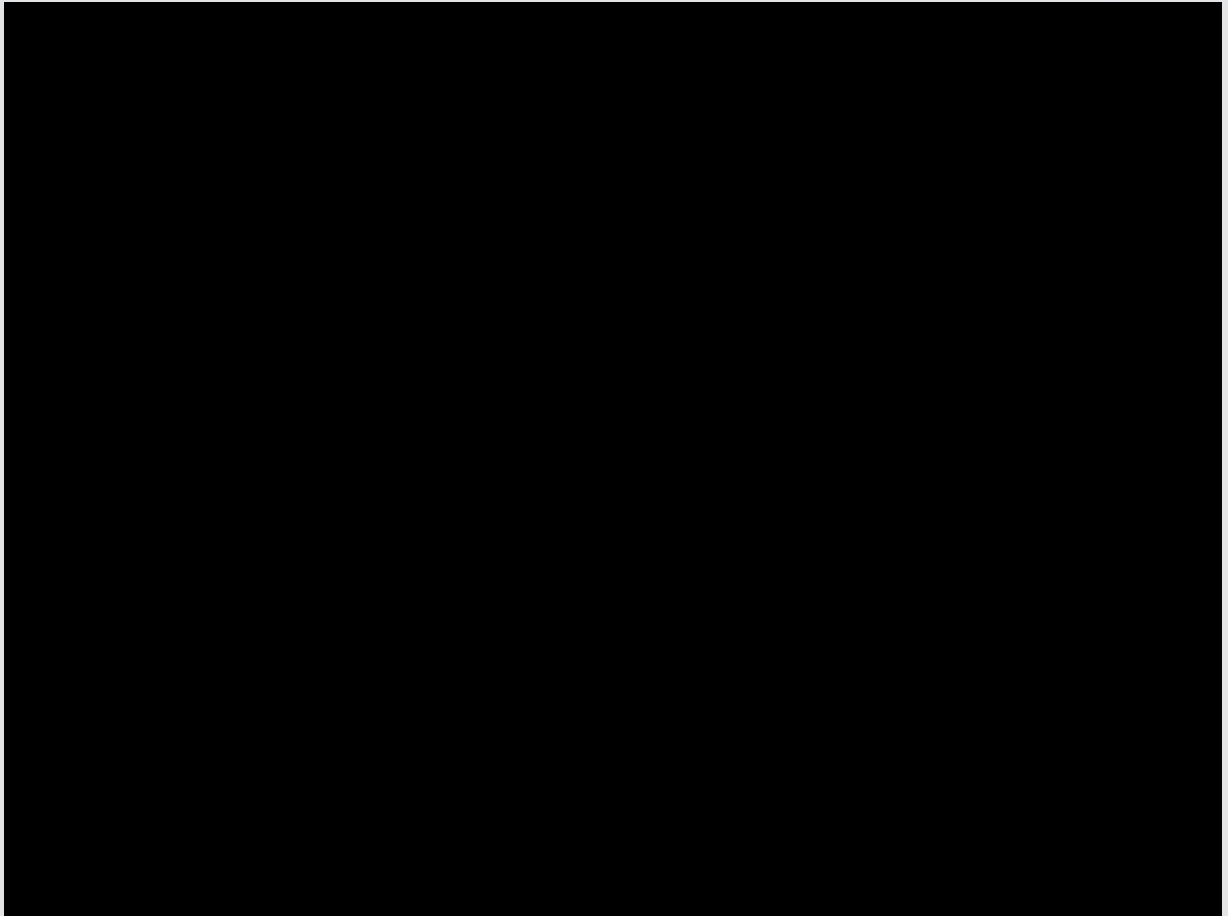
Note: All Yahoo internal host names and image names has been sanitized for all demos.

Image signature check

- Signature makes integrity and publisher verifiable.
- Existing templates build/sign/publish images.



Demo: signature check



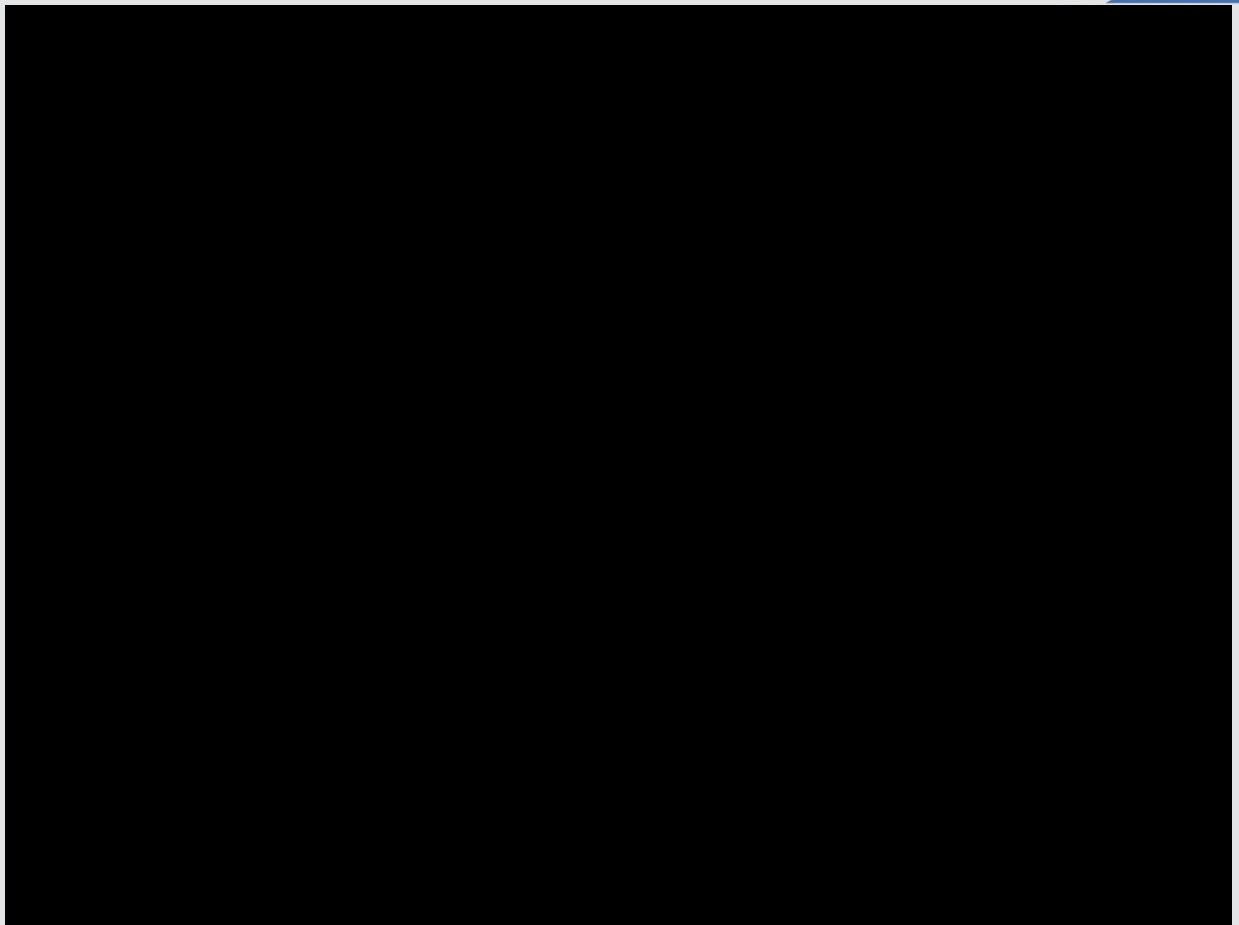
Note: All Yahoo internal host names and image names has been sanitized for all demos.

Image freshness check

Reject stale images.

- Update images regularly.
- Decrease the patch delta.
- Ensure a working build pipeline.

Demo: freshness check

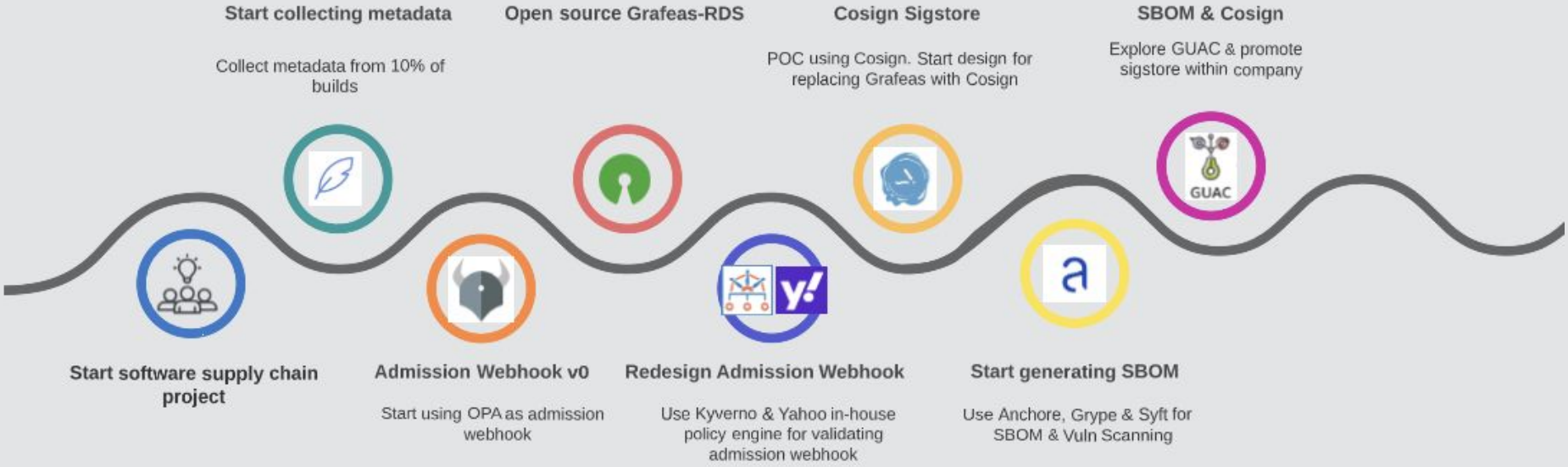


Note: All Yahoo internal host names and image names has been sanitized for all demos.

More deployment verifications

- Vulnerability check.
- Disallow images with latest tag.
- Check pre-defined labels.
- …

Our journey




WHAT DID WE LEARN?

Lessons learned

- Enhance existing developer workflows automatically and by default 
- Pre-plan for adoption & enforcement 
- Visibility of the project 
- Embrace open-source technologies 
- Continuous feedback 

Thank You

Special thanks: Nate Burton, Sean Sposito, Aditya Mahendrakar

Please scan the QR code above to leave feedback for this session