



CONTAINER FACTORY FOR AEROSPACE & DEFENSE

Sarah Miller Melissa Robertson

CLS24582058

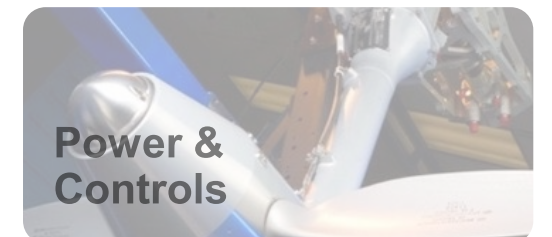
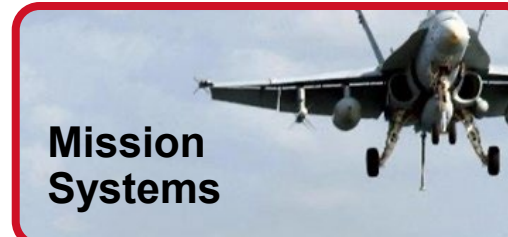
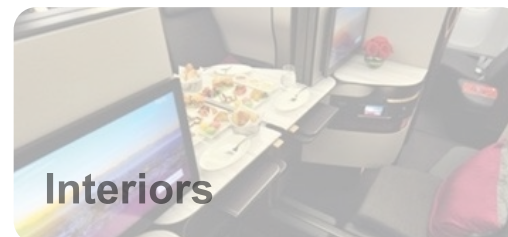
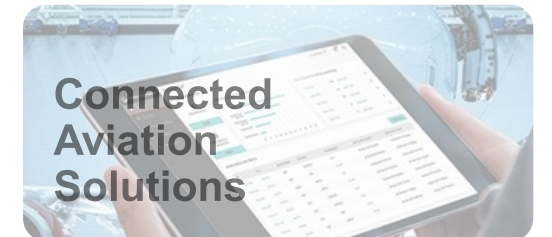
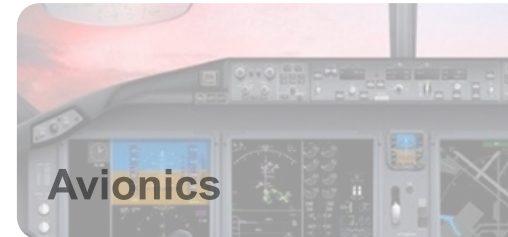
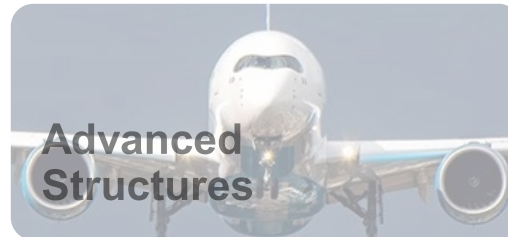
COLLINS: WHO WE ARE



Sarah Miller
Sr. Technical Fellow

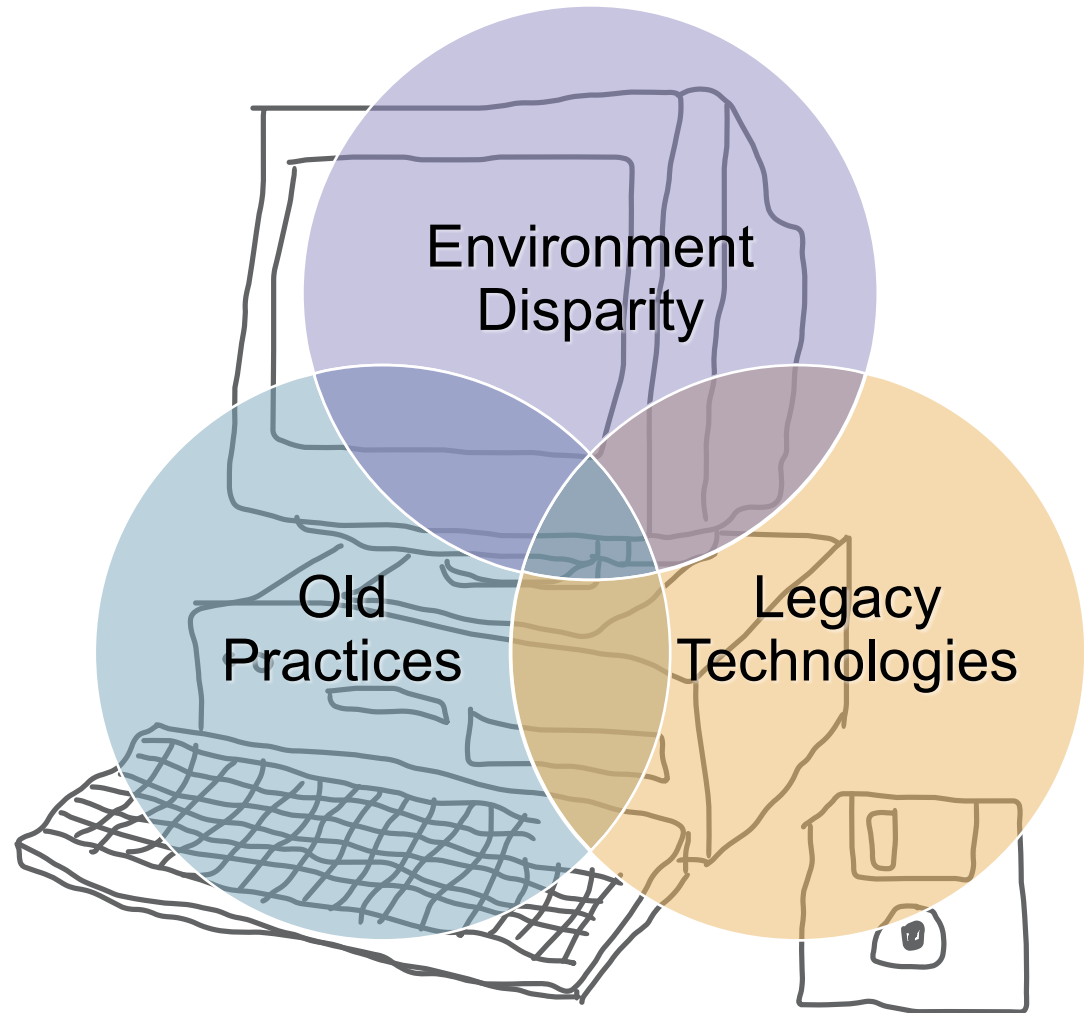


Melissa Robertson
Sr. Software Engineer



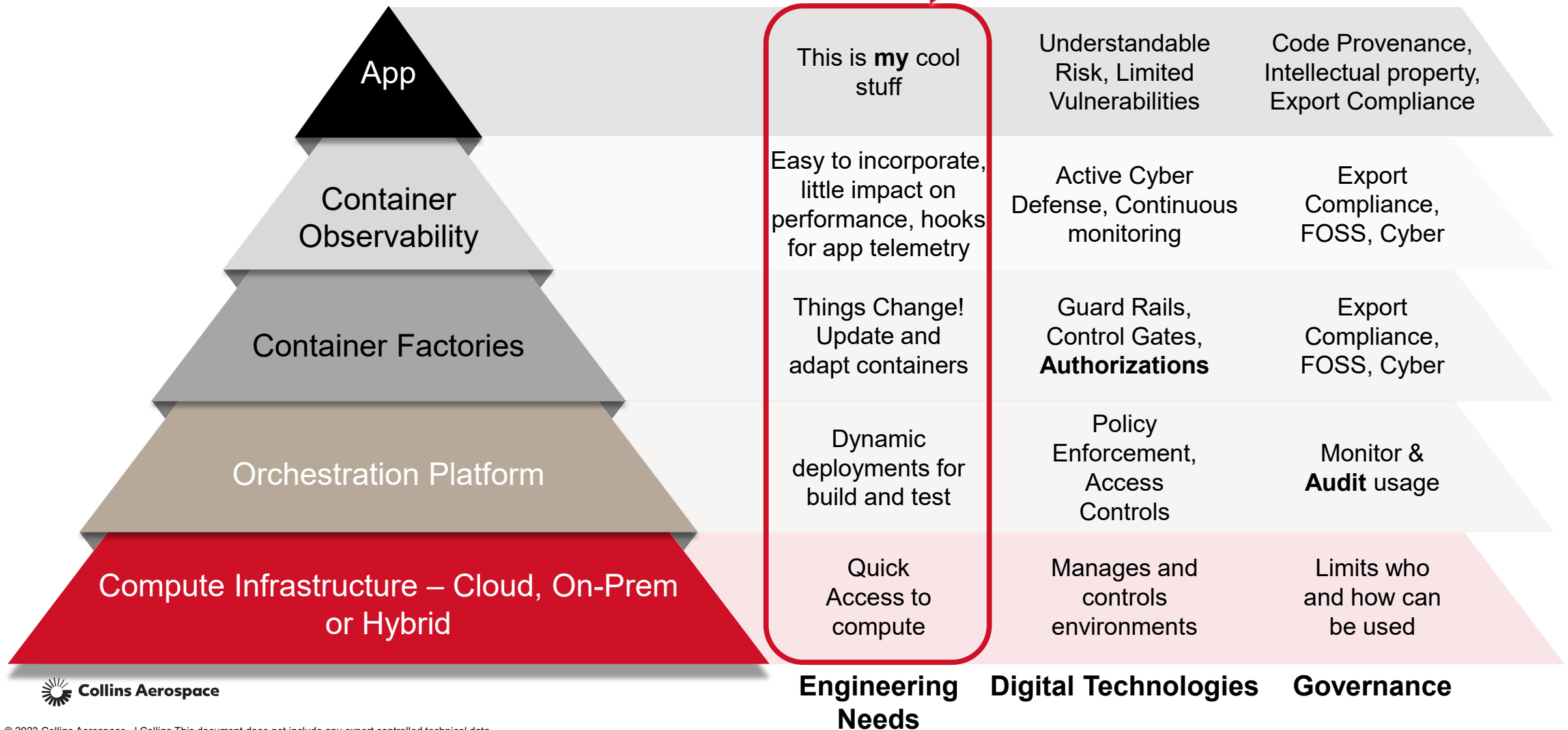
THE PROBLEM

- How do you sustain/maintain products that are 25-30 years old?
- It built/ran on that other server? Why not here?
- Bill said I'd find it on the floppy... I don't know what that is!
- What do you mean there's no bash? (ksh anyone?)




Transformational thinking: Declarative ephemeral build environments

CONTAINER STACK



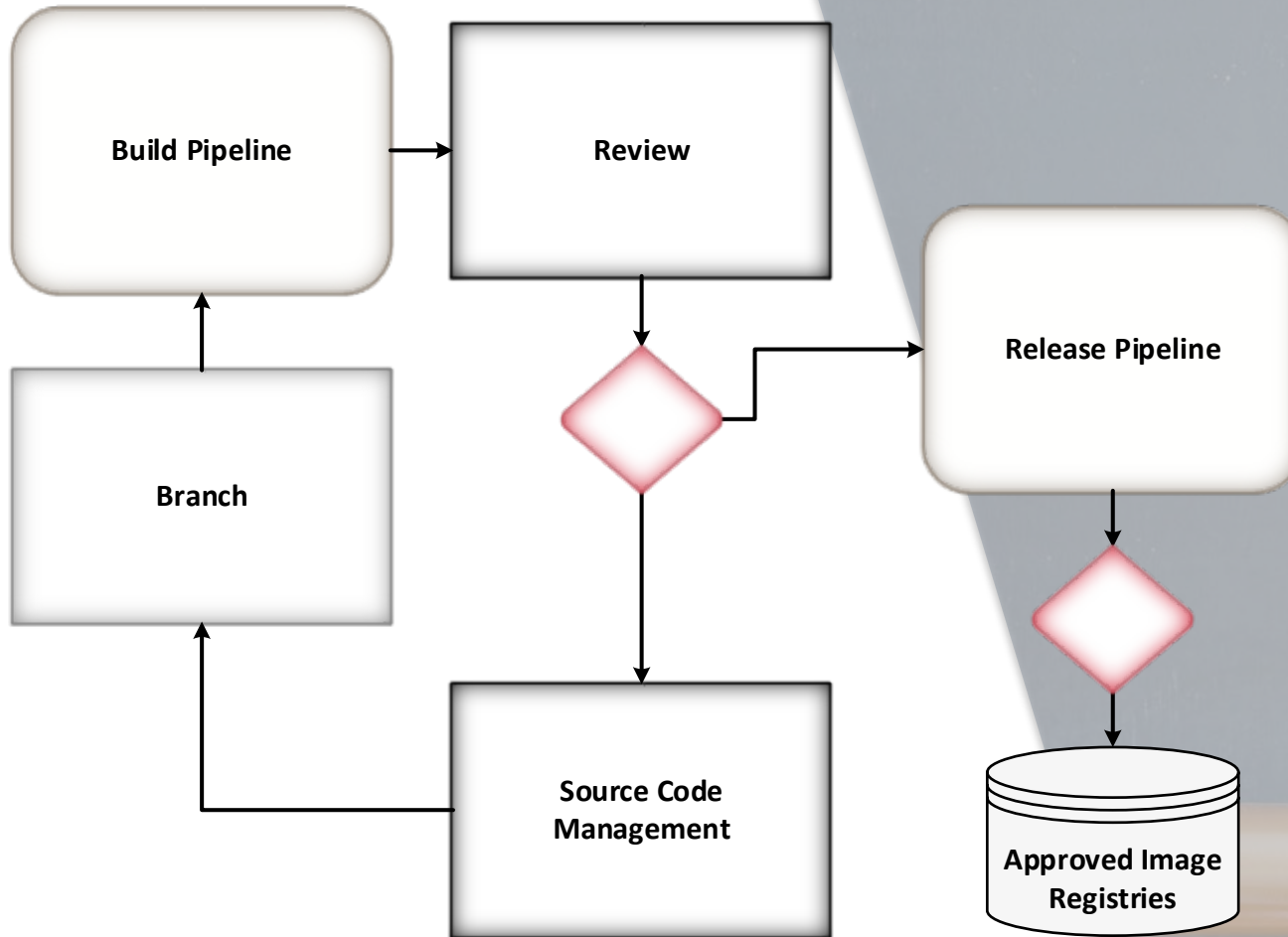
DEVELOPER EXPERIENCE

- Self-service environments
- Reduce cognitive load through automated policy/procedure compliance
- Automate immutable audit record collection
- Curated pipeline stages/jobs/controls
- Standardized container factory



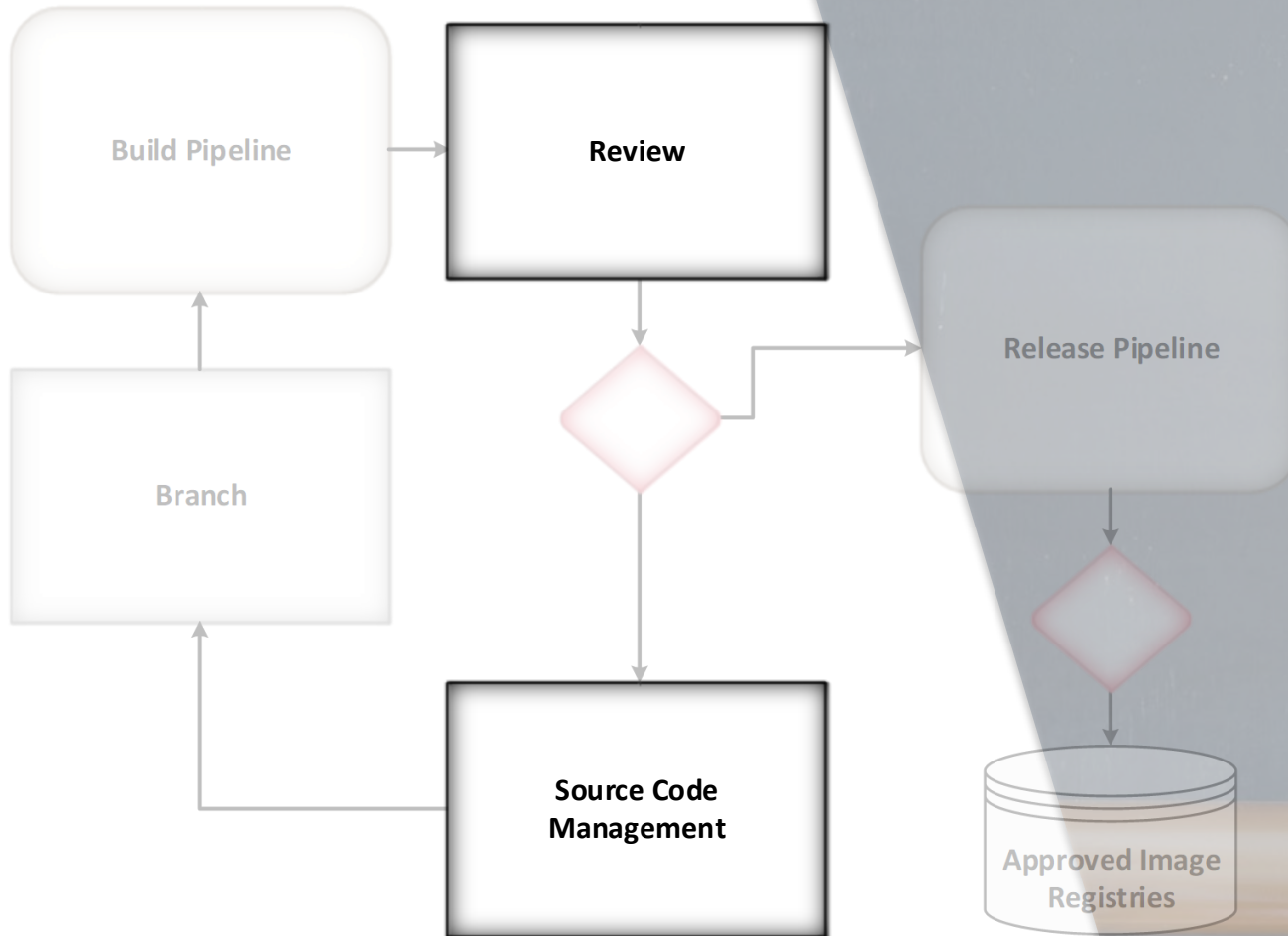
Pathways of least resistance

DEVELOPMENT WORKFLOW



- Separate out controls based on enterprise needs versus customer needs
- Thresholds agreed upon by teams working with quality and security

DEVELOPMENT WORKFLOW



- All source code must be version controlled.
- Requires code attestation
- Code must have two-person peer review

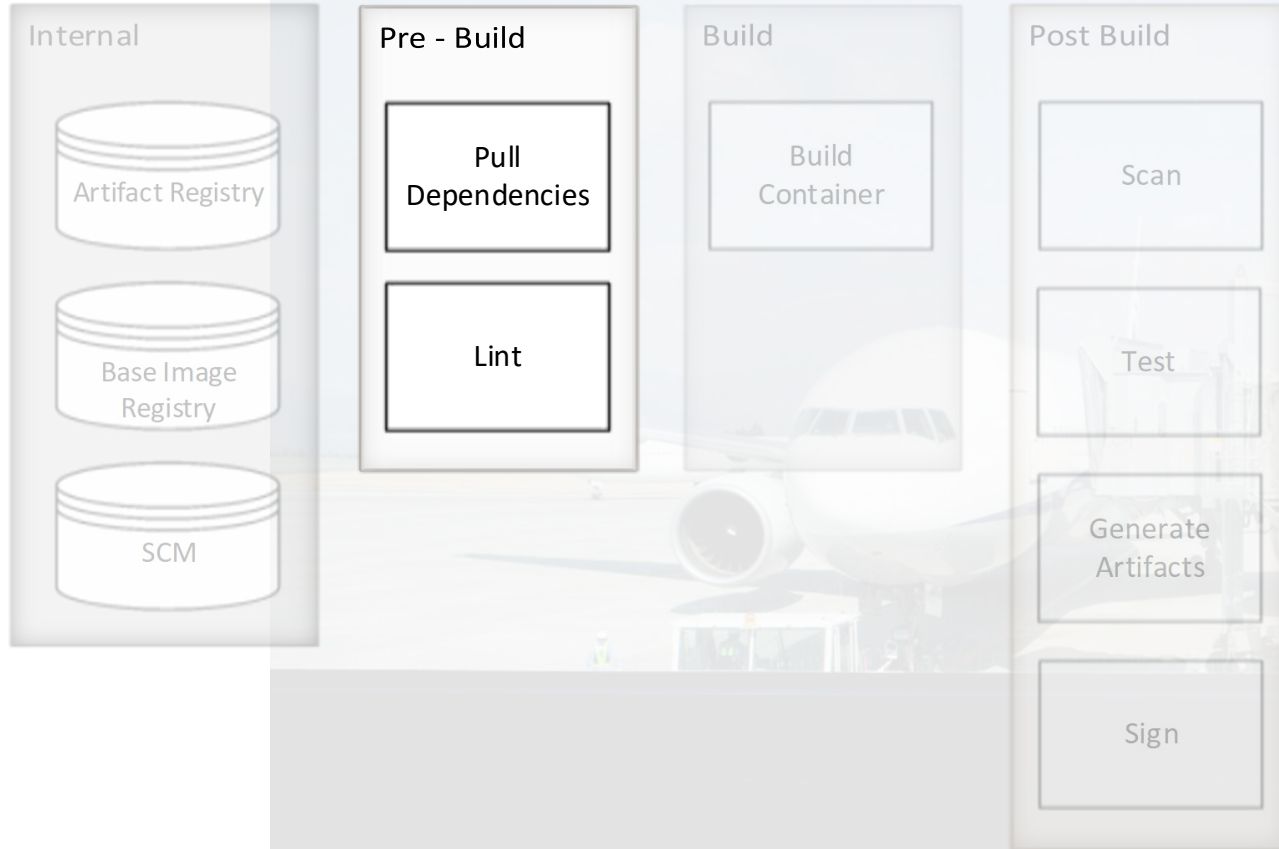
BUILD PIPELINE



Internal Registries

- Approved images and dependencies must have real-time vulnerability scanners.
- Retention policy enabled to purge old images.
- Provides licenses for dependencies used.

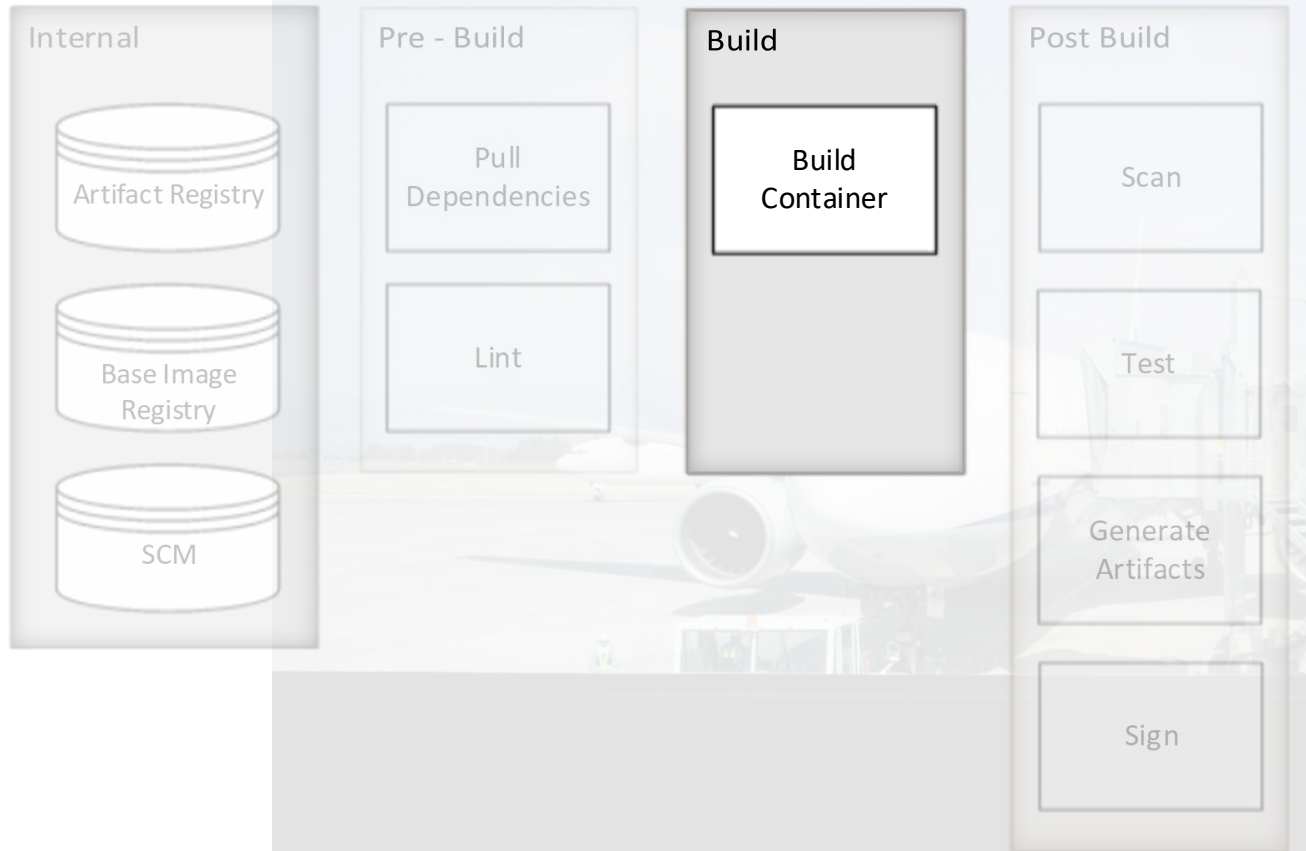
BUILD PIPELINE



Dependencies and Linting

- Build pipeline to pull dependencies and base OS images from and internal approved repository.
- Enforce linting on container creation file.
- Linting allows control over container creation file based on program's needs and corporate policy.

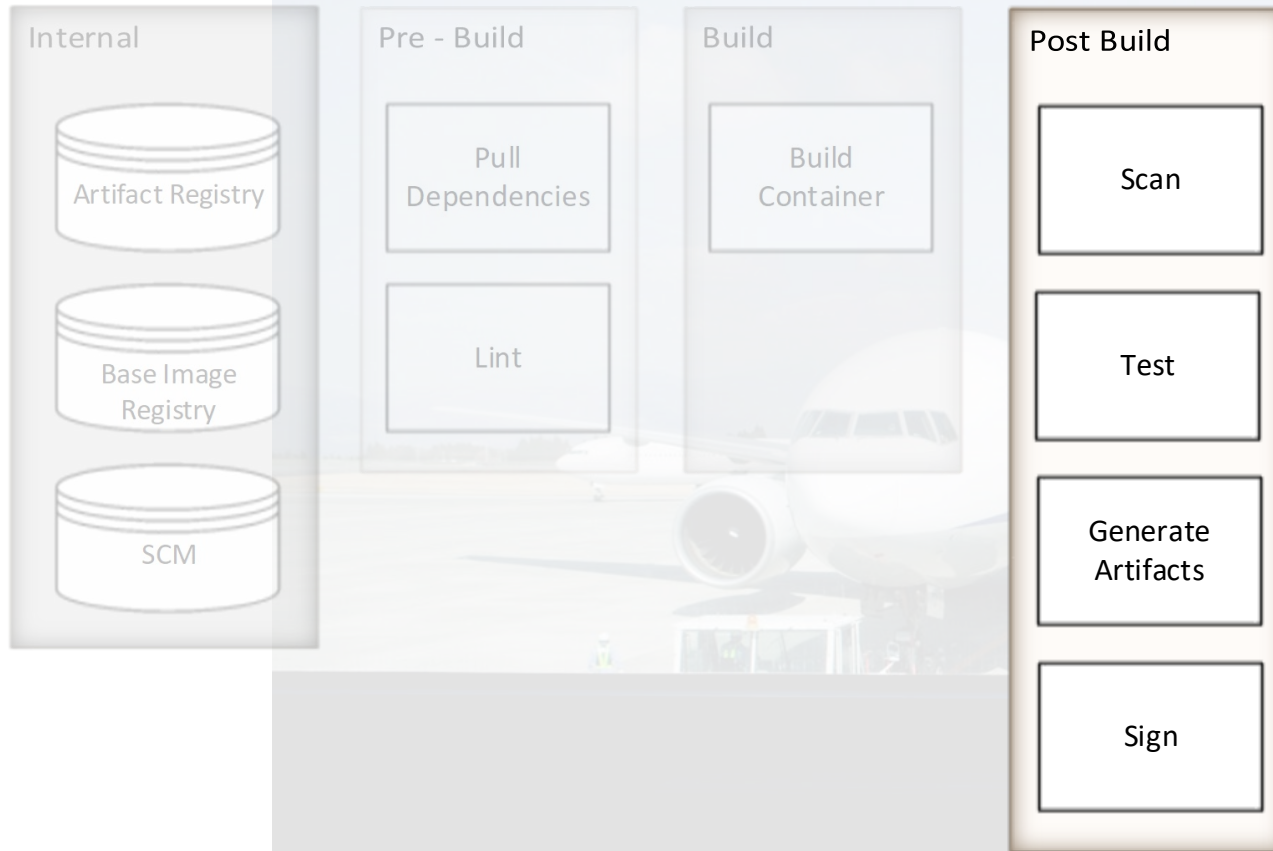
BUILD PIPELINE



Container Build

- Environment must be protected from un-authorized access
- Build system must provide full audit log
- Build process must be automated

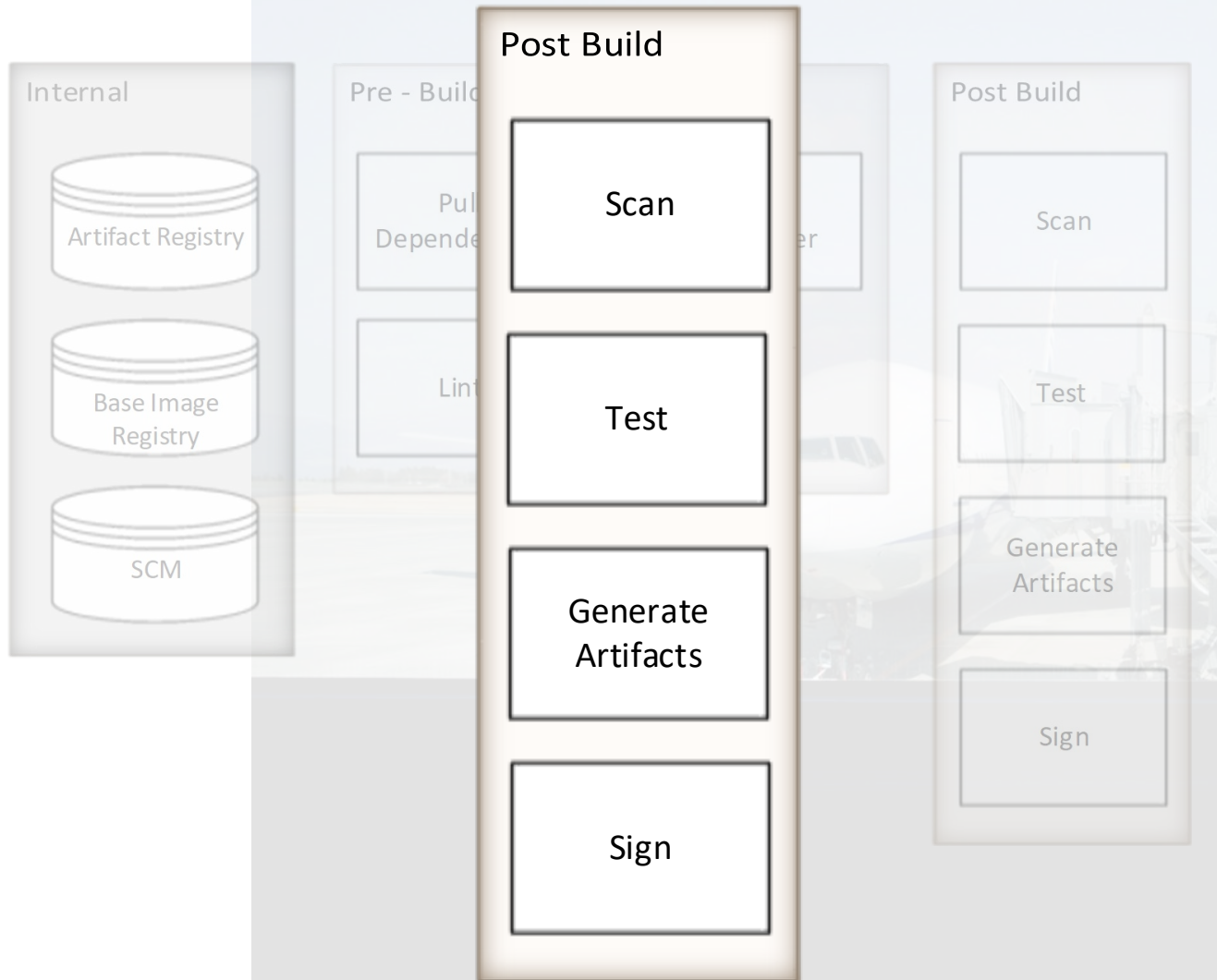
BUILD PIPELINE



Scan

- OS must continue to have Security Technical Implementation Guide (STIG) compliance
- At a minimum 2 vulnerability scanners
- Software Bill of Materials (SBOM) must be generated

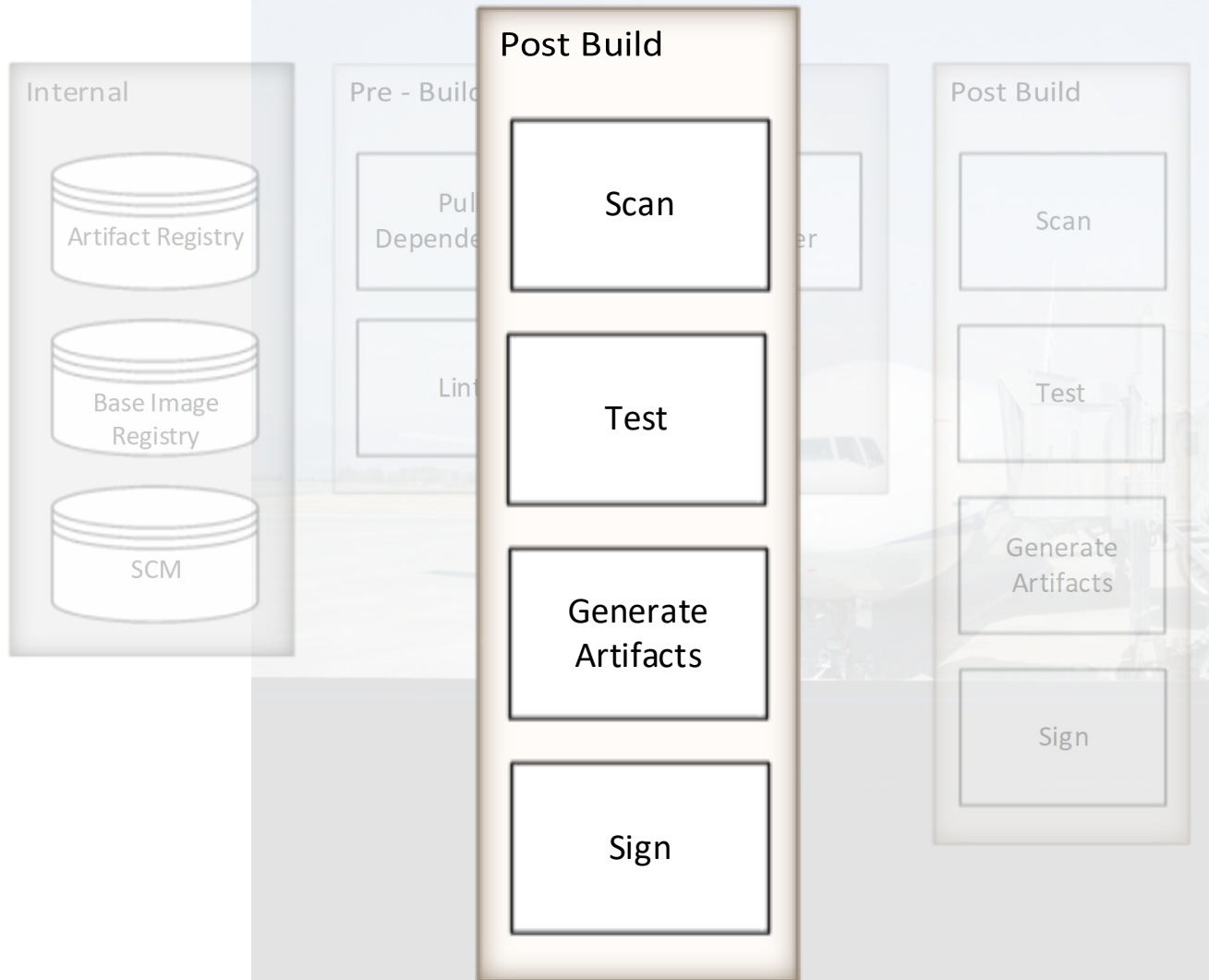
BUILD PIPELINE



Test

- Penetration Testing
- Integration Tests

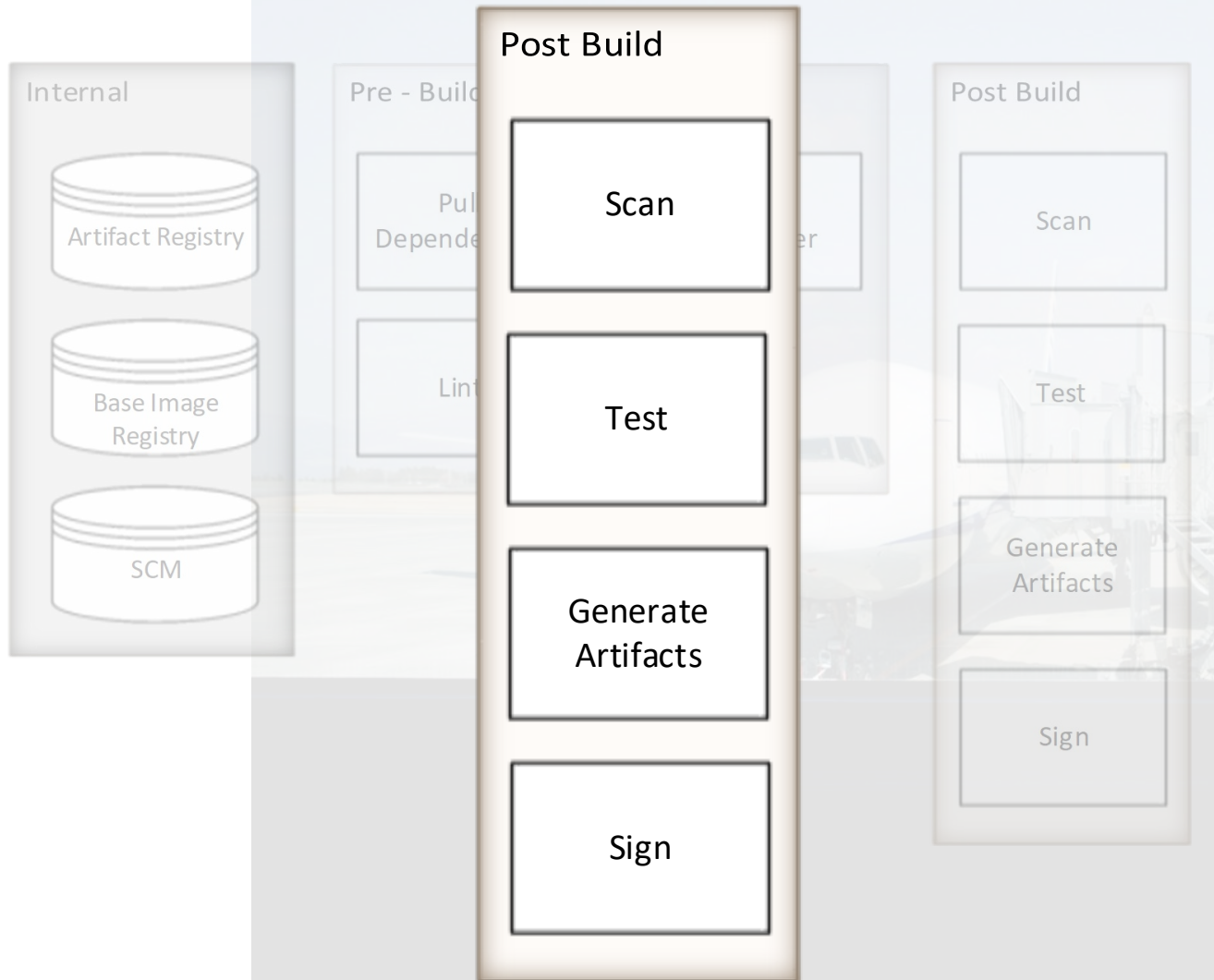
BUILD PIPELINE



Generate Artifacts

- Export Compliance
- FOSS licenses
- Global Trade
- Audit logs
- Rebuild instructions

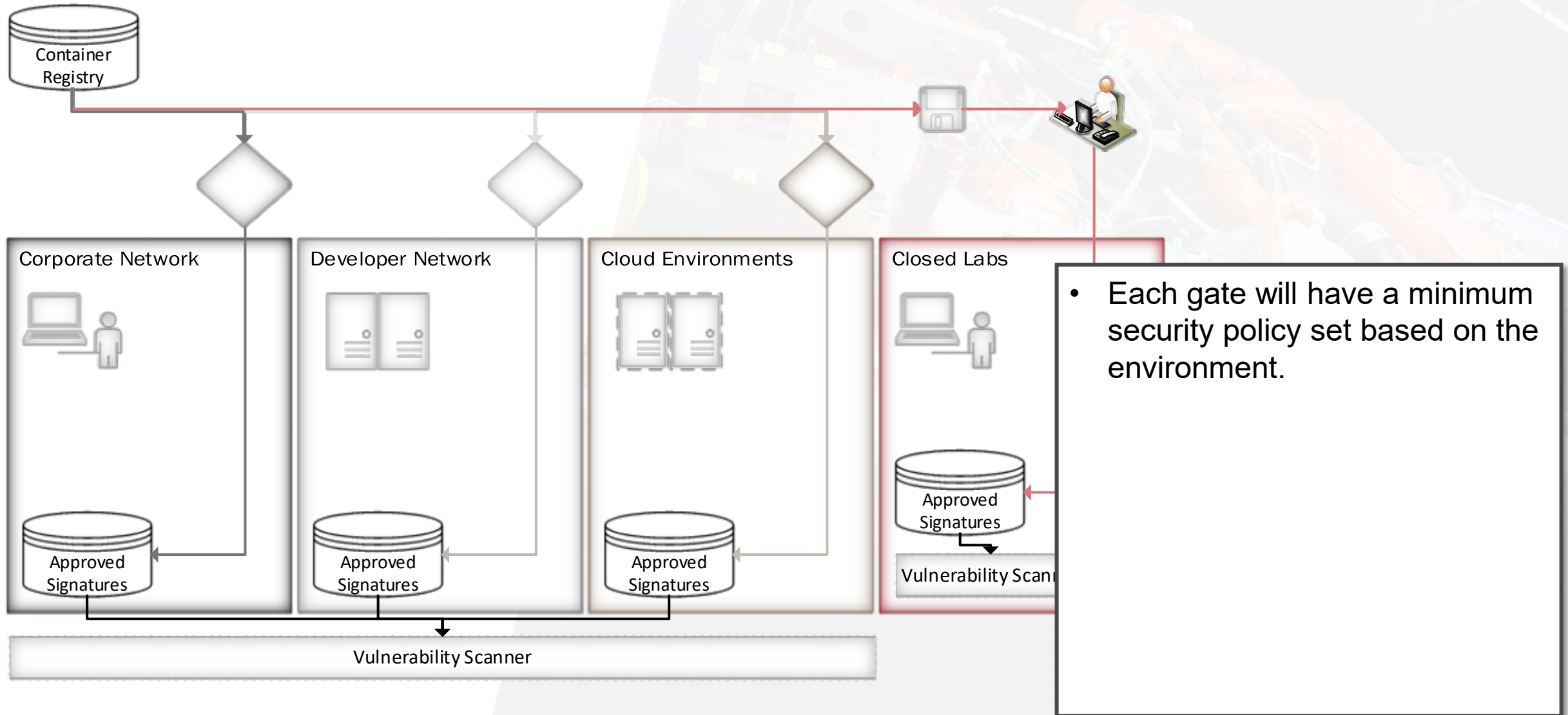
BUILD PIPELINE

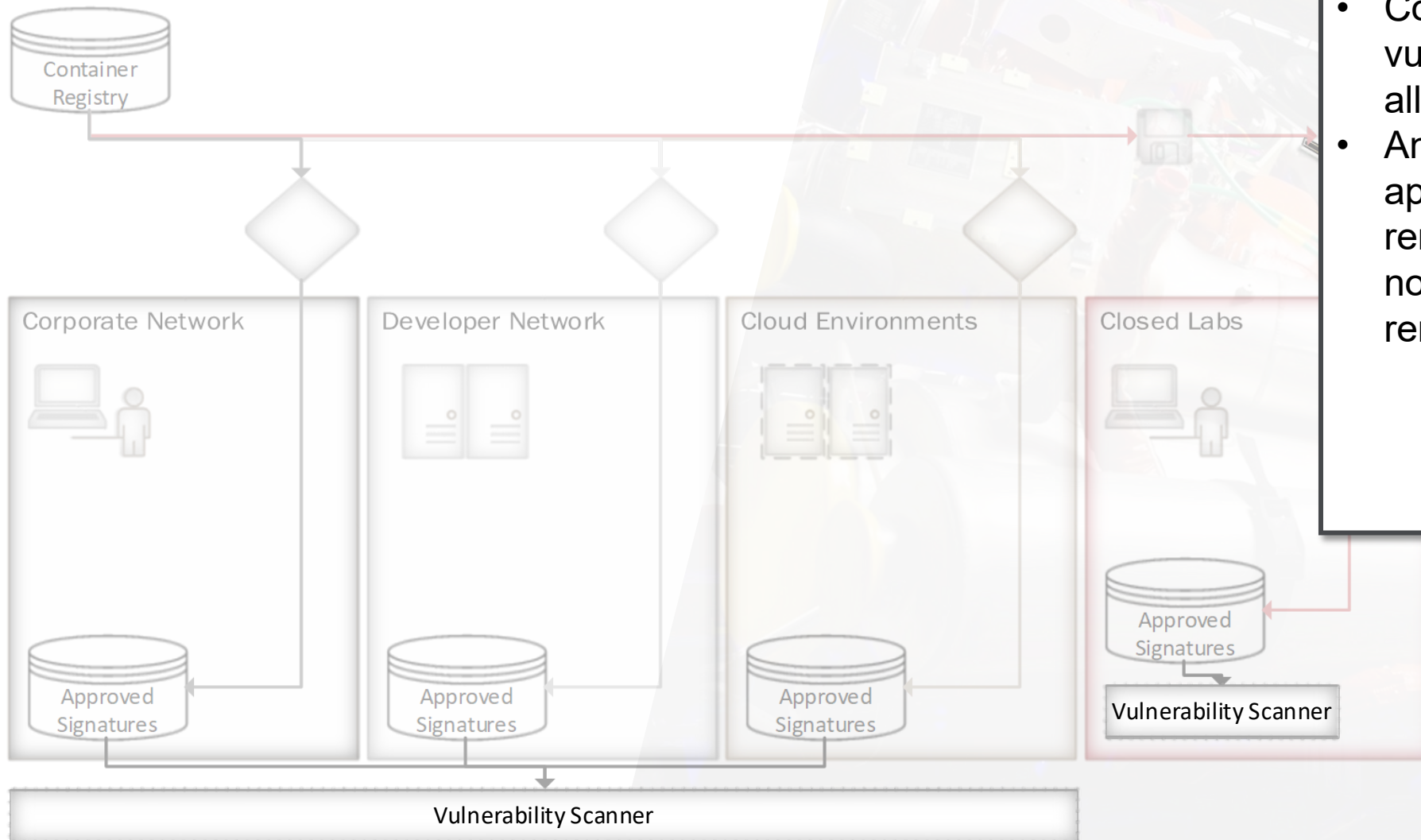


Sign

- Pipeline to leverage authorized certificate for signing.

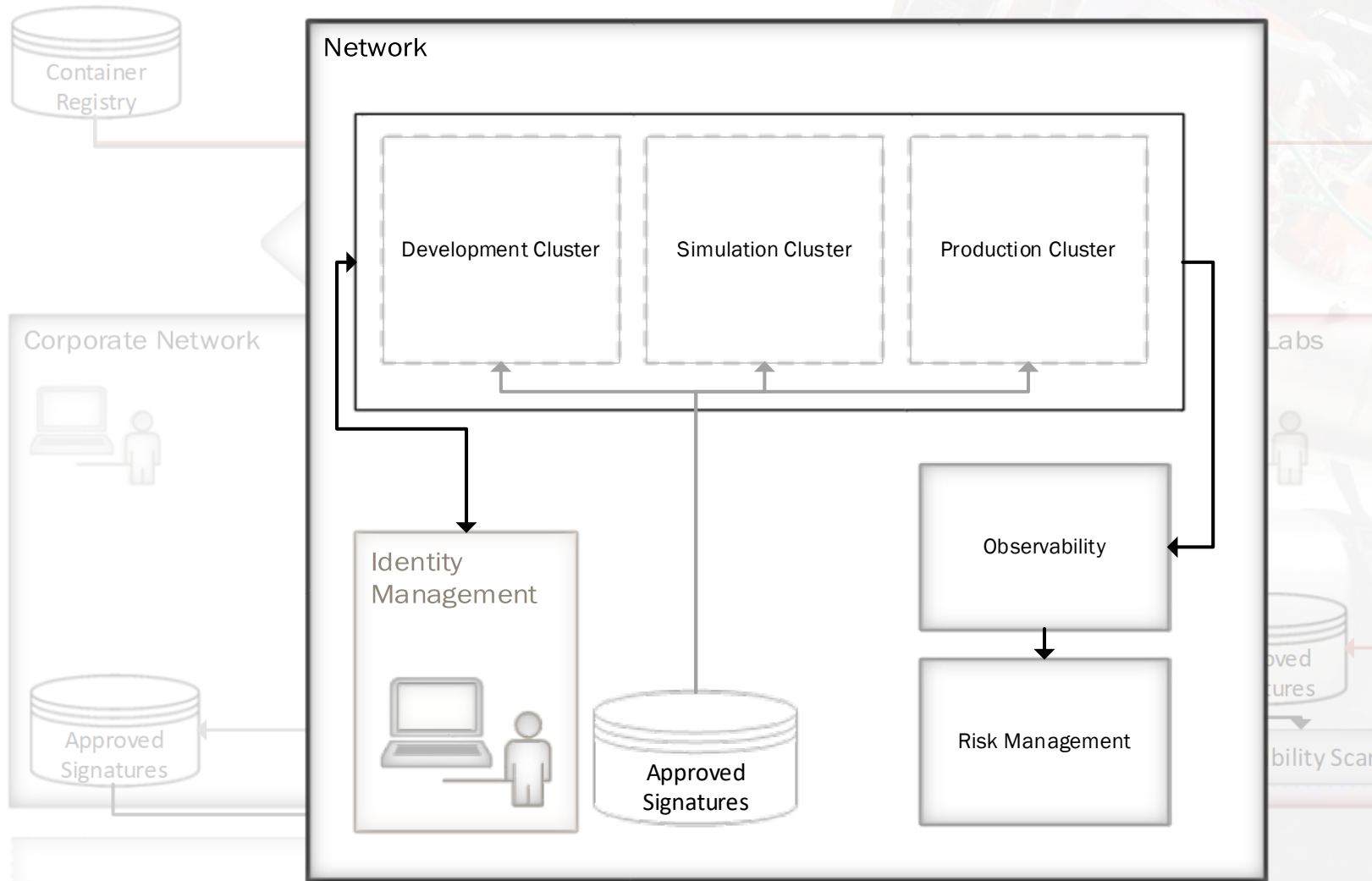
RELEASE PIPELINE





- Continuous scanning for new vulnerabilities must be done for all environments.
- Any scan failure must result in approved signatures being removed, the authorized admin notified, and a ticket created to remediate the threat.

POST PIPELINE



- Enforce boundaries around containers
- Infrastructure needs to be secure enough to put source code in these environments

THANK YOU

- Questions?

