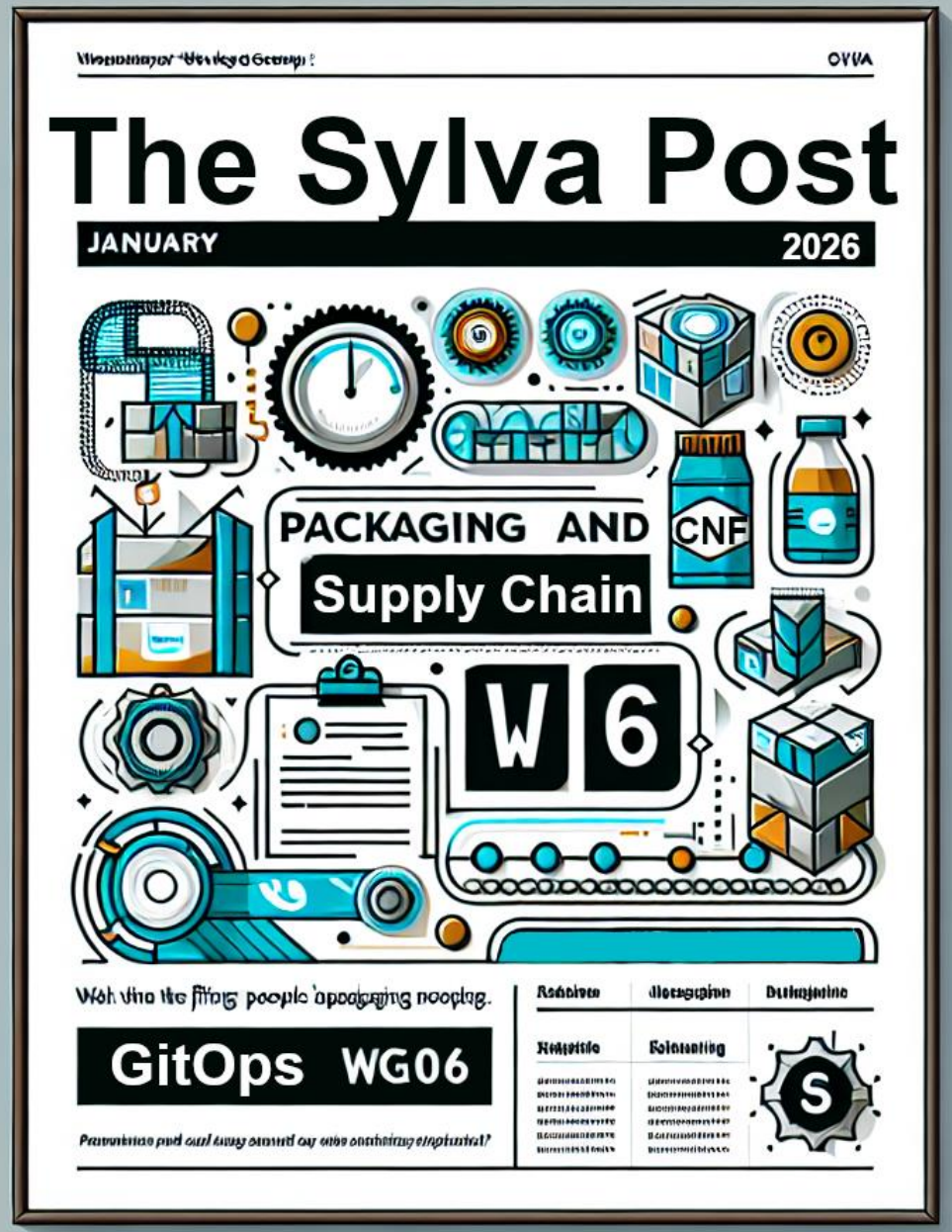


Imagined by you, generated by Dinootoo

January 2026

CNF packaging
(Whitestack/Orange)

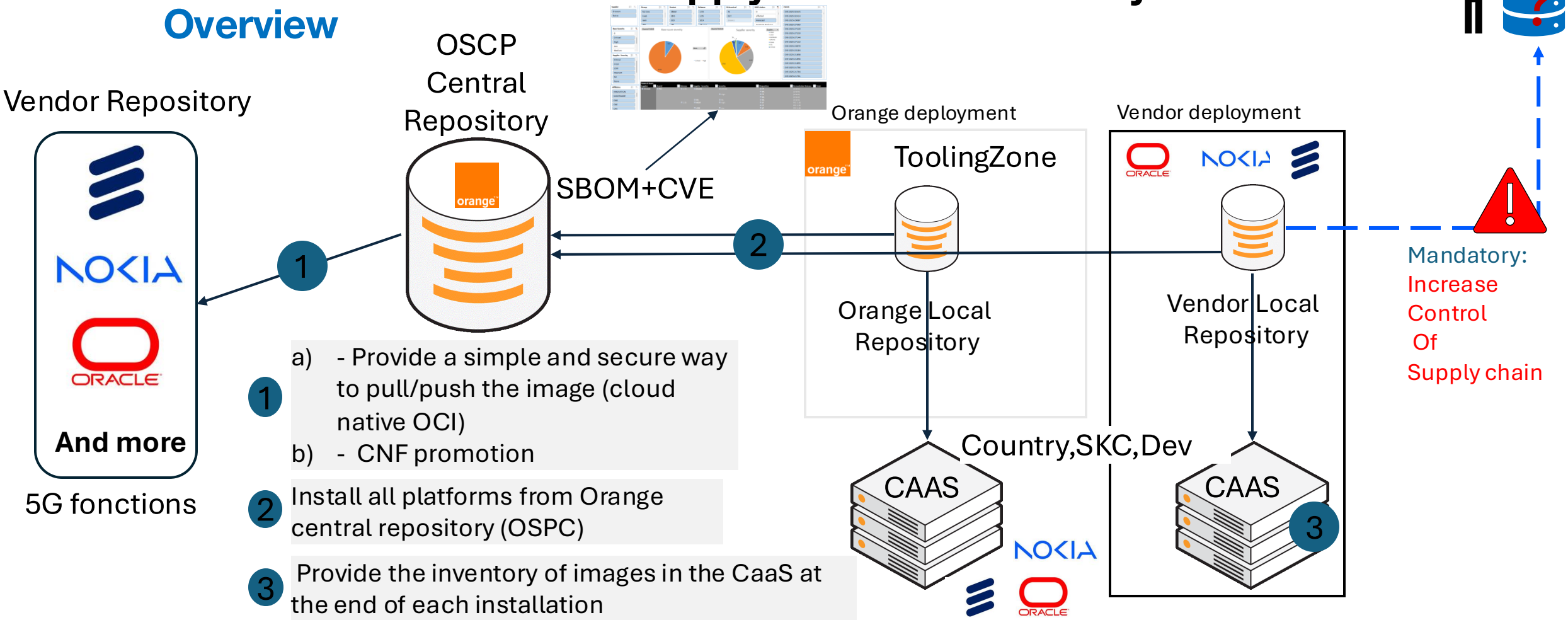
Packaging a CNF in Sylva Unit

Back on Supply Chain

- Starting from WG06 guideline on software Delivery Guideline
- Stakes: collecting OCI artifacts from vendor is still very inconsistent (registry, tar.gz, local registry through professional services)
- Problem: nightmare to precisely know which images are run in which environment and precisely know the system impacted by a new CVE
- Running continuous audit on all production systems is not acceptable
- Basic security mechanisms are not applied (signature)

CICD architecture to secure the supply chain ‘CNF delivery’

Overview



Orange request

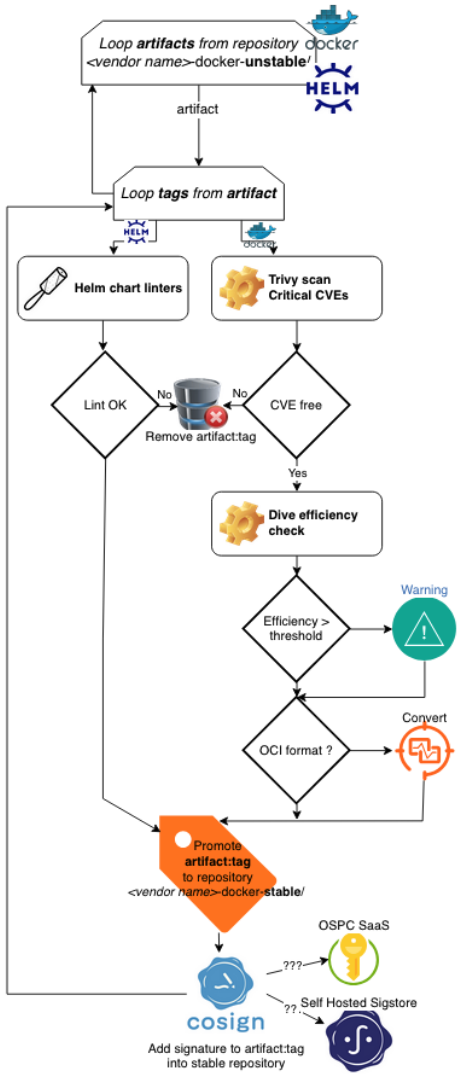
- ❑ **Reminder: Conform to Orange CICD proposed : Install from OSPC (Orange Repo.Tech.Orange)**
- ❑ **Provide inventory of installed artefacts**

OSPC = Orange Software Production Chain

Stage 1a: collect the OCI artifacts

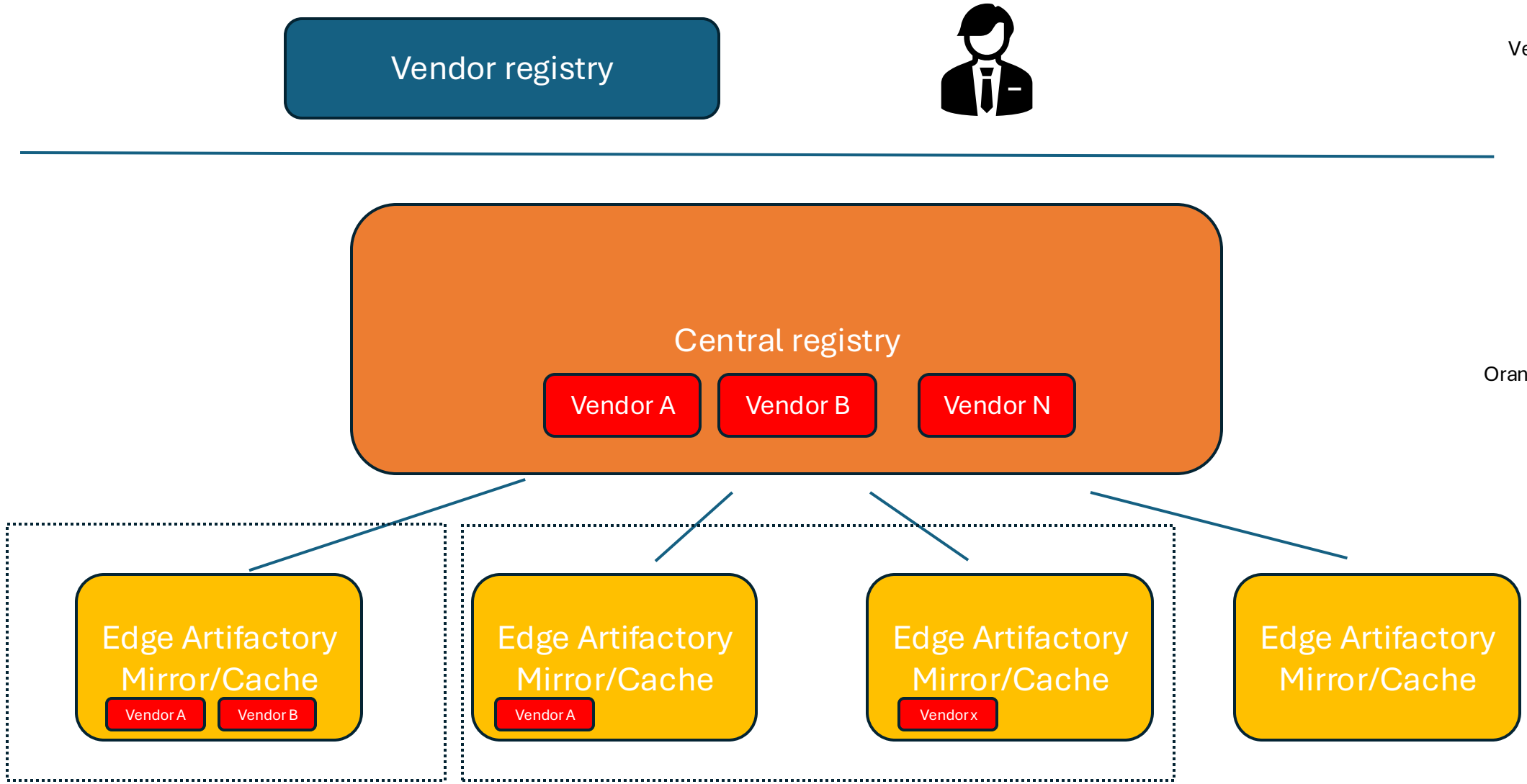
- Central Orange point = JFrog artifactory reachable on Internet (white list)
  - Option 1:Recommended delivery: mirroring towards vendor public registry (already possible with some vendors): automated synchro between vendor registry and Orange registry (token protected)
  - Option 2: Grant an access to an untrusted project to the vendors with IP whitelisted access from Internet (helm push and docker push done by Vendors on orange central Registry)

Stage 1b: Image promotion

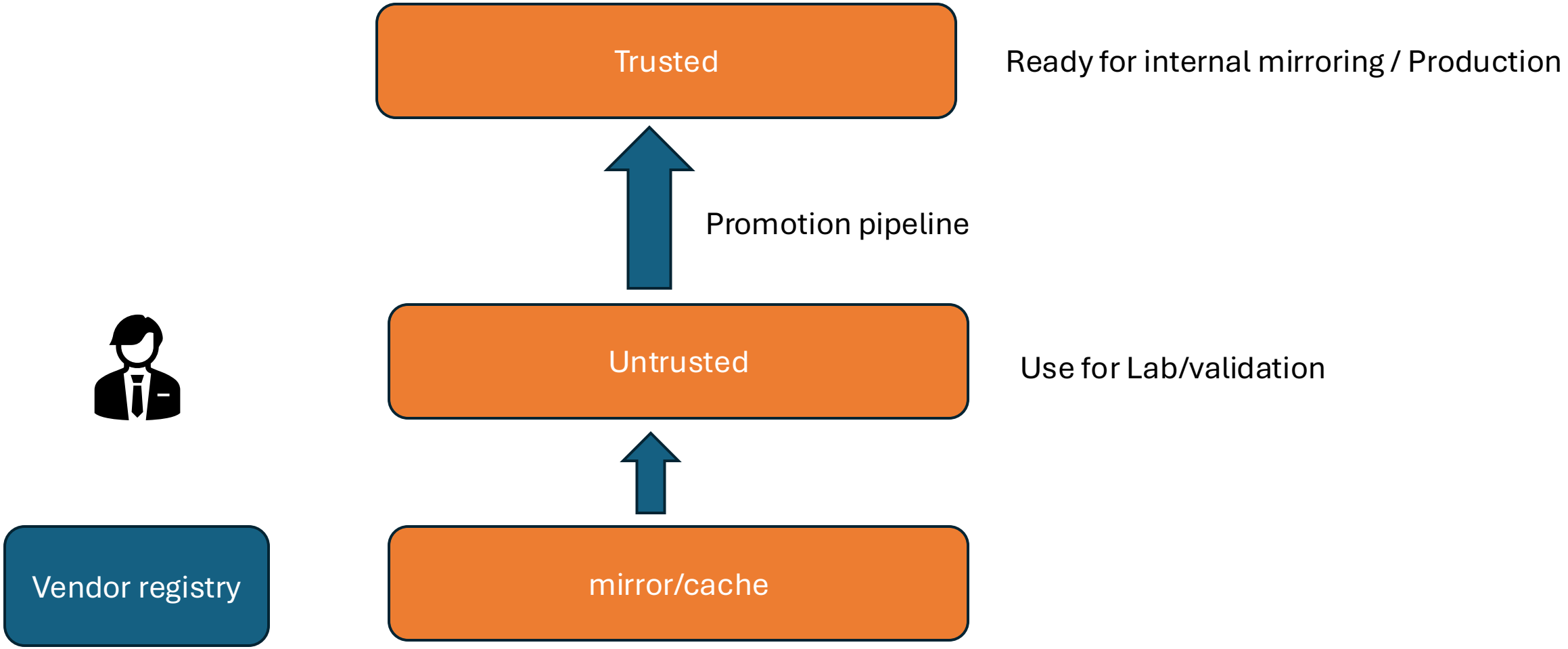


- Helm linting (yaml parser)
- CVE scans (Trivy) including **OpenVex** (vendor when available) and validation team
- Installation **SigStore** NIF TZ to sign images with **Cosign** tool (Innovation, vendors?)
- OCI format check
- Image efficiency

Stage 1: Multi vendors / Multi countries



Stage 2: control, promote and give feedback



Stage 3: images inventory, centralized scans