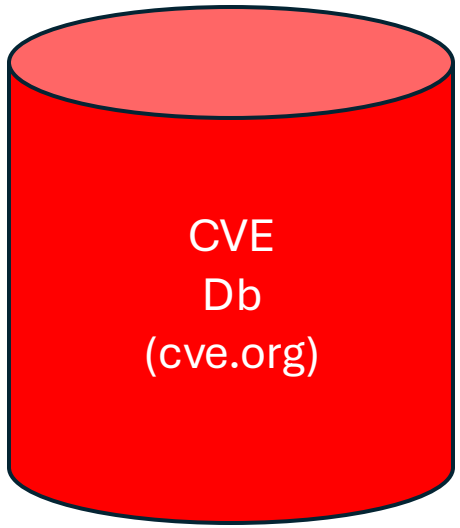
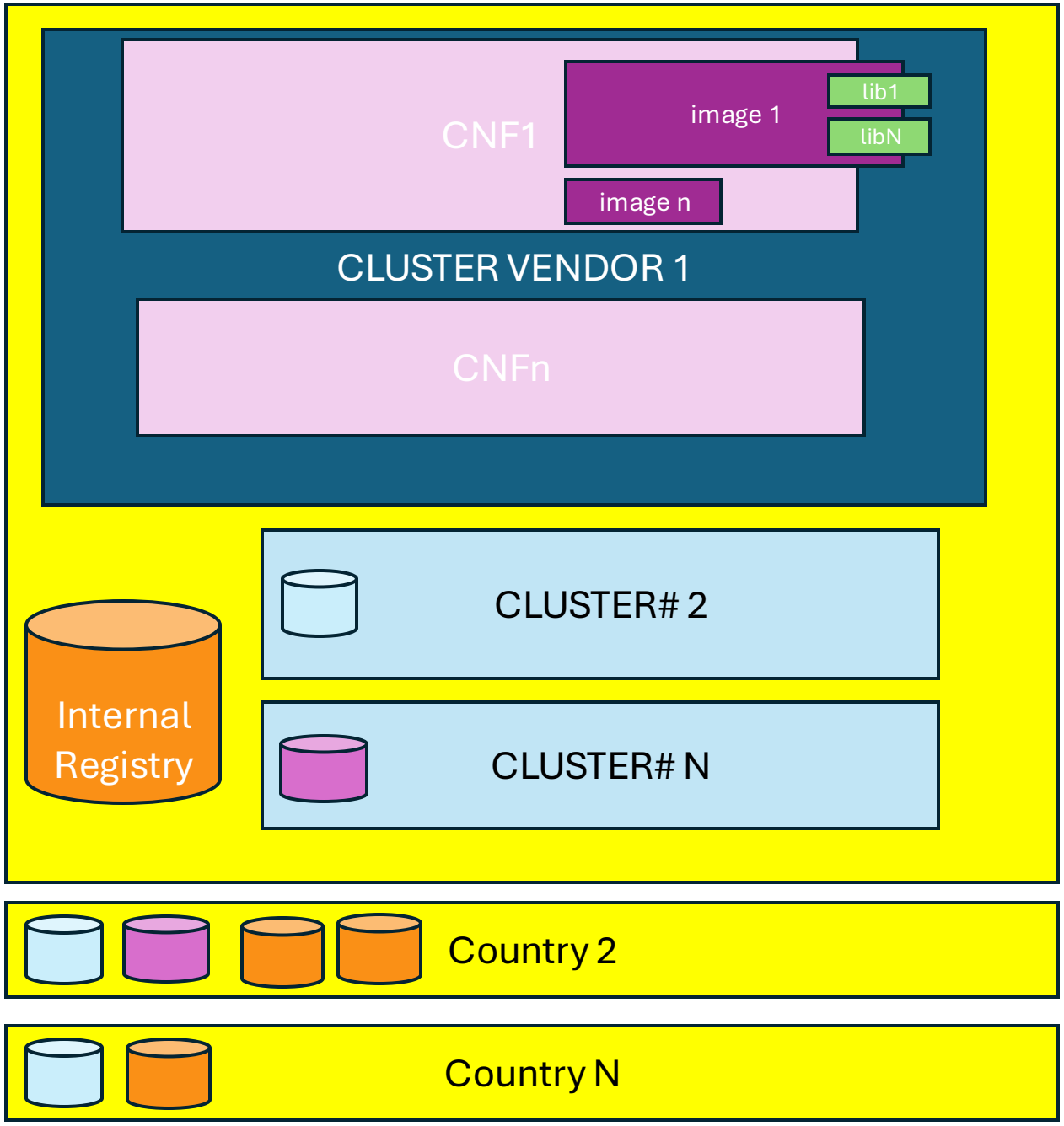
https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

5G Core CVE

CVE CNF 5G





Software ate the world, so did CVE

NIS2 raised questions

- A new critical CVE is declared
  - Give me the list of all the impacted systems: Country / Site / NF / docker / image / layer
  - What is the plan to fix it: CNF vendors / Infra vendors / Open Source communities
  - Prove that we did everything we can to fix the CVE

NIS2 consequence

- We need an inventory of the OCI resources with good granularity
- We need to be able to locate where the CVE is present
- We need to secure the sofware supply chain
- We need to be able to audit our systems anytime anywhere

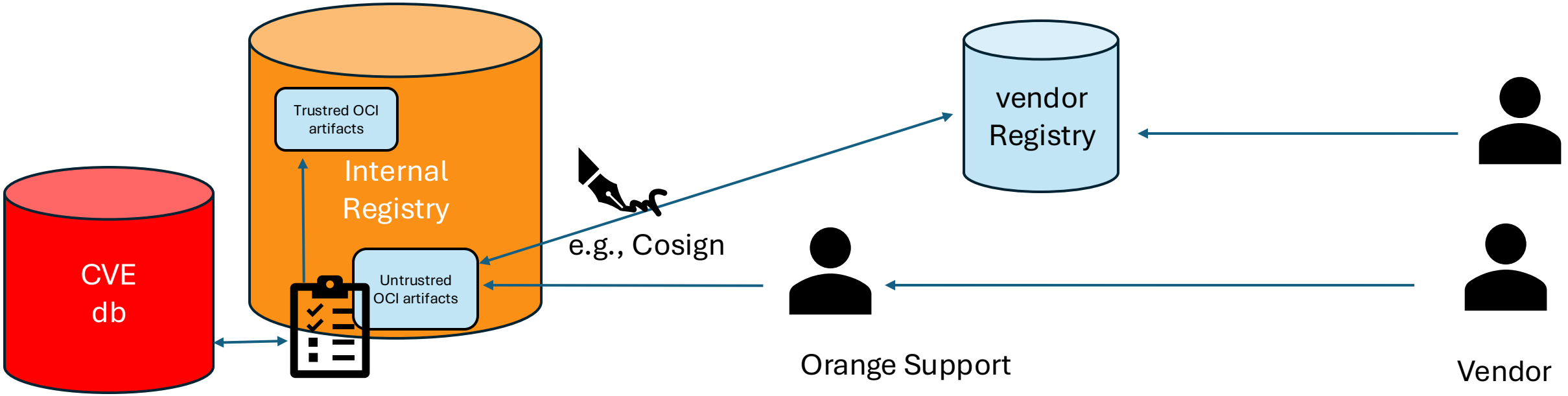
How do we address that

- It is an Infra problem
  - forward the question to WG1 (infra and security) and WG3 (security)
  - Scan baby scan => keep on scanning all the clusters (not very efficient, not very green..)
- For a CNF deployed with GitOps, let's consider it can be a GitOps problem
  - Find a programatic way to list the resources and compare these resources with CVE

CVE /NIS2: How to get the list of sites/clusters impacted by a new CVE?

- Hypothesis
  - CNF deployed through our GitOps engine
  - CNF vendor images pulled in an Internal telco central registry (very optimistic…)
  - Resource capability to perform CVE scans (Trivy, anchor, xray,..)
  - Dashboards to track CVE are available (dependency track, Defect dojo,..)
  - We do not want to keep on performing security scans on Production instances

1- Scan any OCI artifact on artifact delivery (before any deployment)

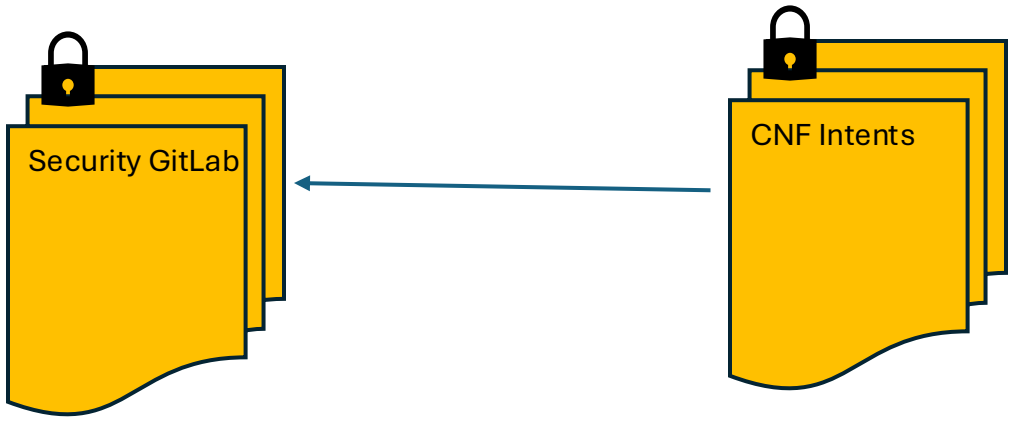


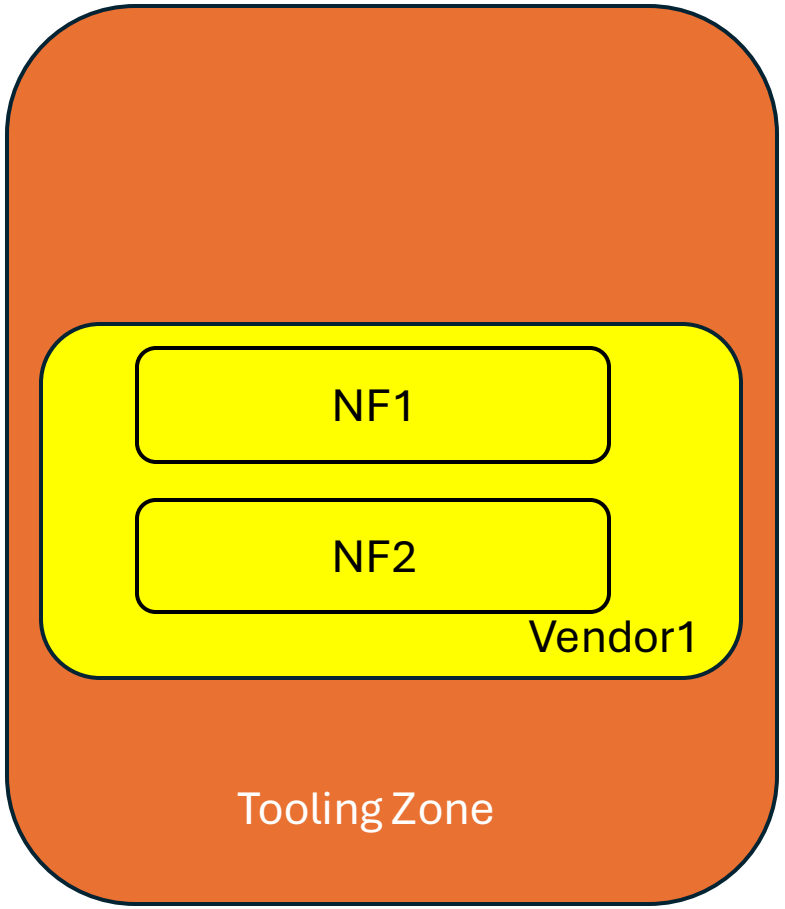
CVE Dashboard

Telco team
- Scans artifacts on Vendor delivery at the first record
- Identifies Critical/High CVE
- Reports to Support/Vendors
- Validates untrusted => trusted

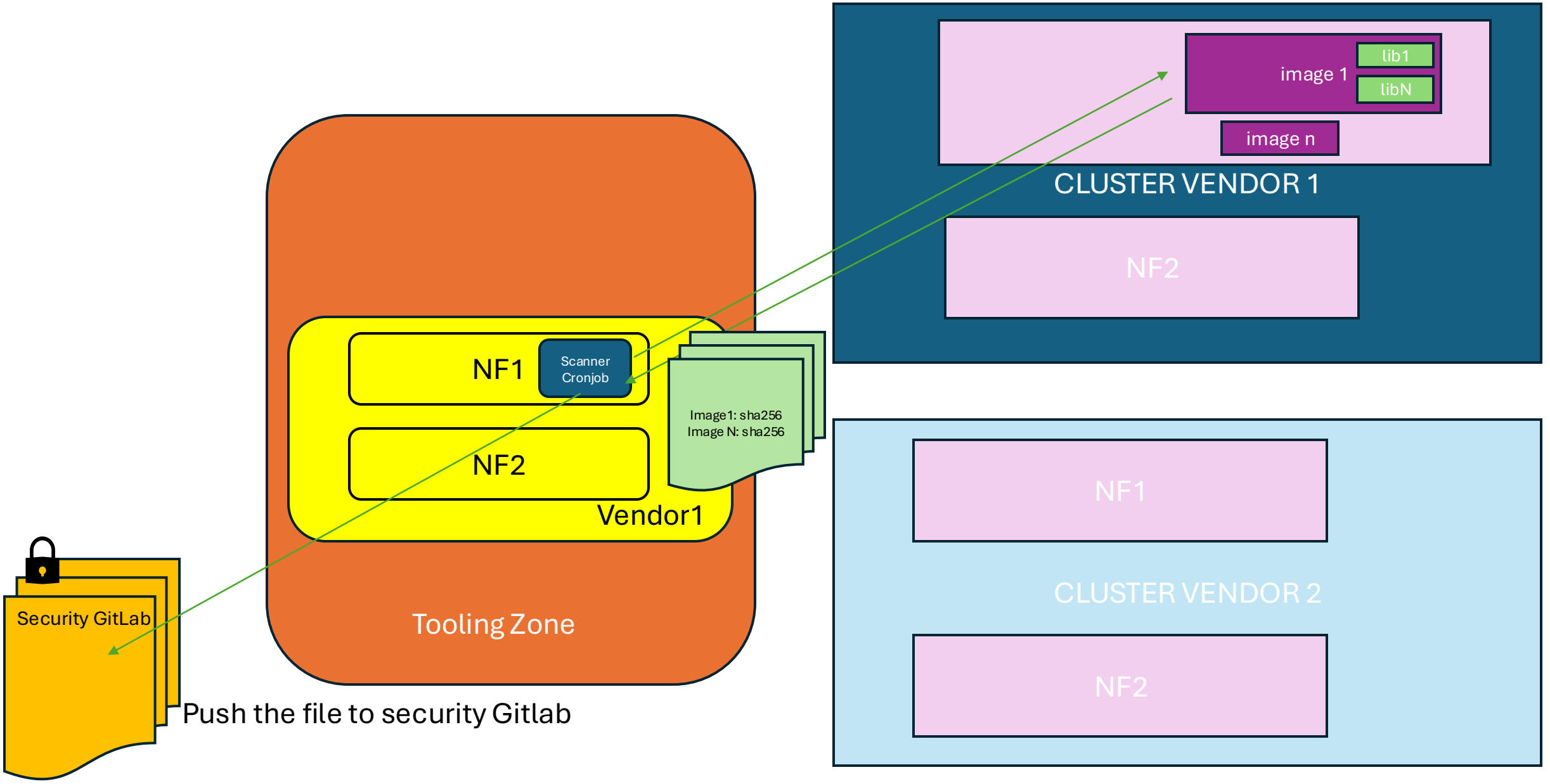
2a: Trust Git

- analyse CNF intents and list all the images
- Provide the list of images to security team
- Telco team checks CVE with ref DB and raises flag in case of match



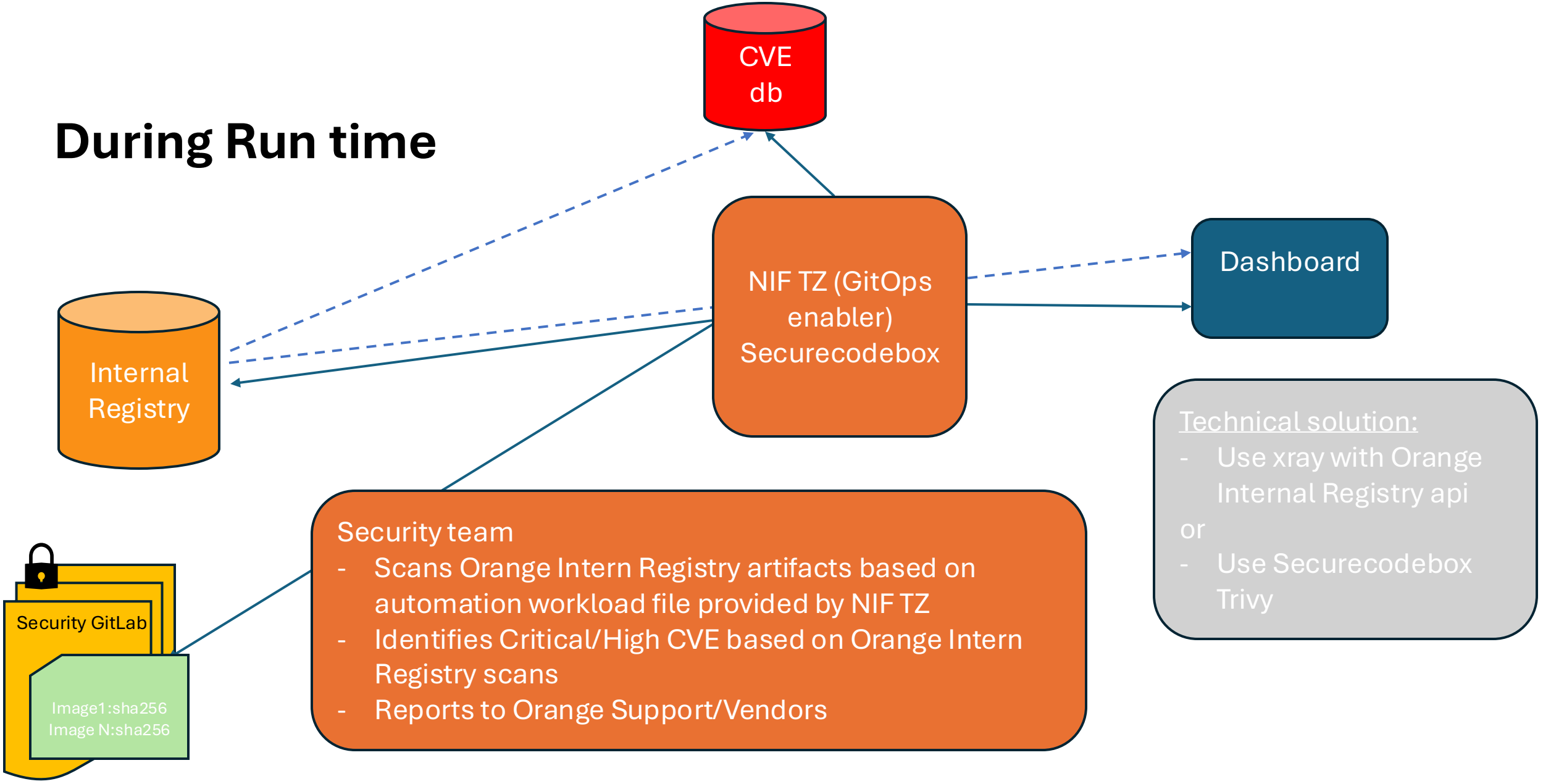


2b: trust only the runtime



Telco Team scan example

During Run time



Issues

- 2a: we missed all the resources created by operators => not acceptable
- 2b: All the images in runtime are not in Internal registry (local registries)..we shall assume that Orange Internal registry is the central delivery and should be stricter on "local" vendor registries
  - Deal with vendors to use exclusively the reference Registry – cf guideline on software delivery guideline
- In some cases we had to change the format before pushing a docker image to the central registry => sha256 changes even if the layers do not change
- Adapt the name of image to get image from local Orange Interne registry Egde (*name of Edge + Cnf Fingerprint or Tag*)