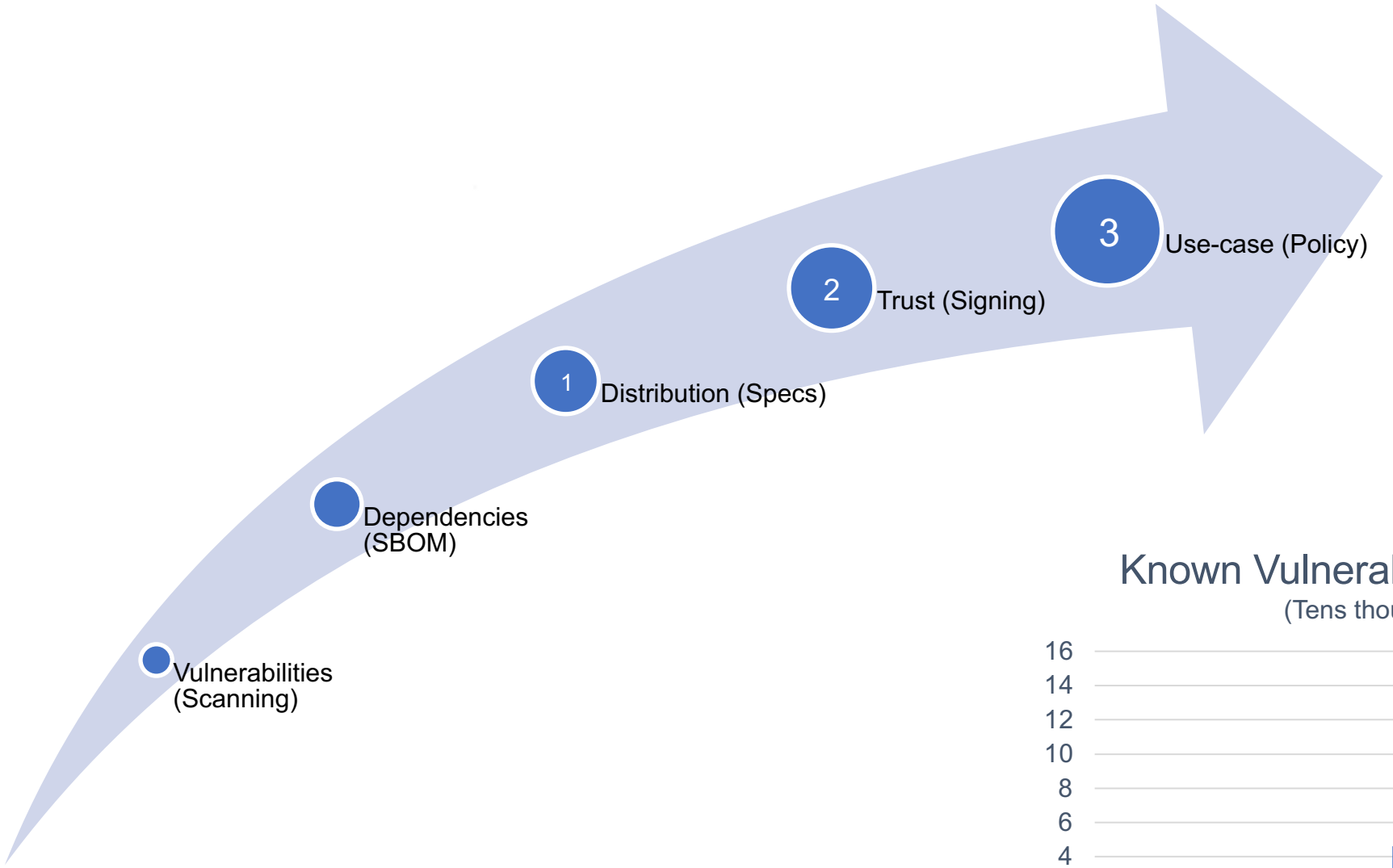

KubeCon
CloudNativeCon
Europe 2023
TiKV

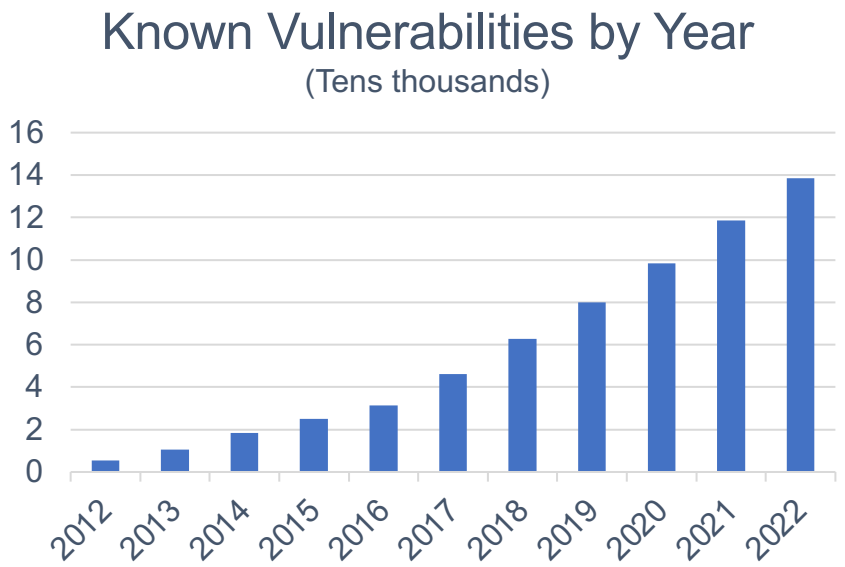
Improve Vulnerability Management with OCI Artifacts - It is That Easy!

Itay Shakury, VP Open Source, Aqua Security
Toddy Mladenov, Principal PM, Azure Containers

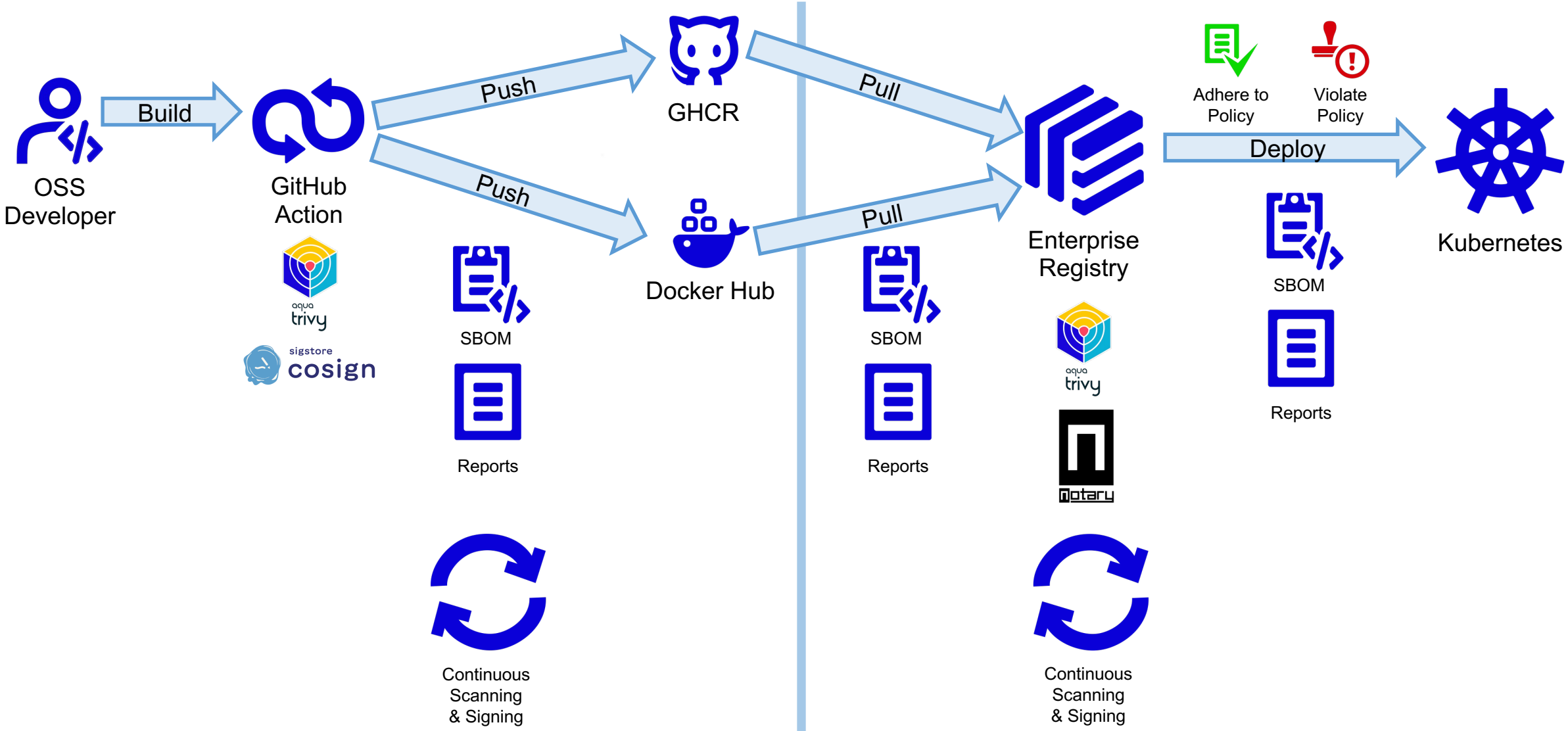
itaysk
toddysm

Agenda


Vulnerabilities (Scanning)
Dependencies (SBOM)
1
Distribution (Specs)
2
Trust (Signing)
3
Use-case (Policy)


Known Vulnerabilities by Year
(Tens thousands)
16
14
12
10
8
6
4
2
0
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022

Use cases


OSS Developer
Build
GitHub Action
aqua trivy
sigstore cosign
Push
Push
GHCR
Docker Hub
SBOM
Reports
Continuous Scanning & Signing
Pull
Pull
SBOM
Reports
Enterprise Registry
aqua trivy
notary
Continuous Scanning & Signing
Adhere to Policy
Violate Policy
Deploy
SBOM
Reports
Kubernetes
Open Source
Enterprise

What Are OCI Artifacts and Referrers?

KubeCon CloudNativeCon Europe 2023

Artifacts

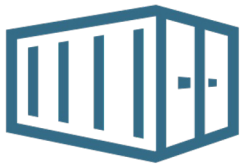
Container Image

Deployment Chart

Signature

Attestation

Referrers



Container Image

Signature

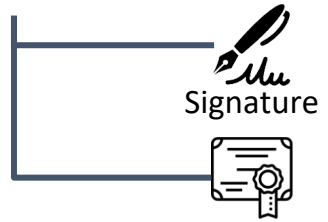
Attestation

Deployment Chart

Signature

Attestation

Container Image



Signature

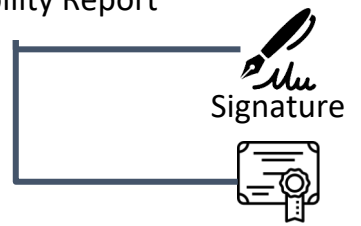
Attestation

SBOM

Signature

Attestation

Vulnerability Report



Signature

Attestation

toddysm

[Modifying the Immutable: Attaching Artifacts to OCI Images - Brandon Mitchel, BoxBoat, YouTube]

Referrer API

KubeCon CloudNativeCon Europe 2023

Endpoints

ID	Method	API Endpoint	Success	Failure
end-1	`GET`	`/v2/`	`200`	`404` / `401`
end-2	`GET` / `HEAD`	`/v2/<name>/blobs/<digest>`	`200`	`404`
end-3	`GET` / `HEAD`	`/v2/<name>/manifests/<reference>`	`200`	`404`
end-4a	`POST`	`/v2/<name>/blobs/uploads/`	`202`	`404`
end-4b	`POST`	`/v2/<name>/blobs/uploads/?digest=<digest>`	`201` / `202`	`404` / `400`
end-5	`PATCH`	`/v2/<name>/blobs/uploads/<reference>`	`202`	`404` / `416`
end-6	`PUT`	`/v2/<name>/blobs/uploads/<reference>?digest=<digest>`	`201`	`404` / `400`
end-7	`PUT`	`/v2/<name>/manifests/<reference>`	`201`	`404`
end-8a	`GET`	`/v2/<name>/tags/list`	`200`	`404`
end-8b	`GET`	`/v2/<name>/tags/list?n=<integer>&last=<integer>`	`200`	`404`
end-9	`DELETE`	`/v2/<name>/manifests/<reference>`	`202`	`404` / `400` / `405`
end-10	`DELETE`	`/v2/<name>/blobs/<digest>`	`202`	`404` / `405`
end-11	`POST`	`/v2/<name>/blobs/uploads/?mount=<digest>&from=<other_name>`	`201`	`404`
end-12a	`GET`	`/v2/<name>/referrers/<digest>`	`200`	`404` / `400`
end-12b	`GET`	`/v2/<name>/referrers/<digest>?artifactType=<artifactType>`	`200`	`404` / `400`

toddysm

https://github.com/opencontainers/distribution-spec/blob/v1.1.0-rc1/spec.md#endpoints

Referrer API Examples

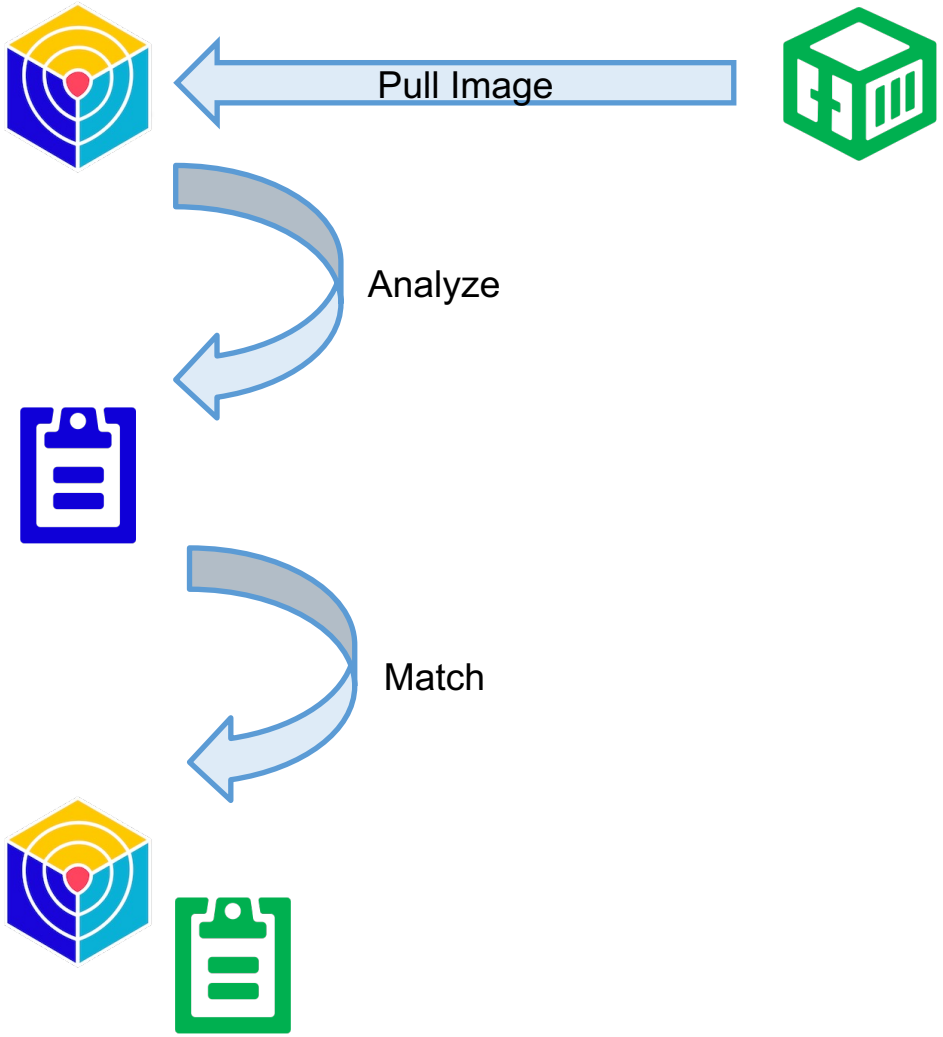
KubeCon CloudNativeCon Europe 2023

```
[ toddysm@tsm-mbp-msft ~ oras discover tsmacrusw3kubeconeu23.azurecr.io/kubeconeu23-python:3.11.2-slim -o tree
tsmacrusw3kubeconeu23.azurecr.io/kubeconeu23-python:3.11.2-slim
├── application/vnd.trivy.vulnerability-report
│   └── sha256:e12f0ce2bf3a06d3f925b0f3e3356f0f22065d5aed2d59a3a5ad3bd76a959f80
├── application/sarif+json
│   ├── sha256:10a663cf824a11c0c7728afc45a036603400ca12a4cdde8a9d71701210981ce5
│   │   └── application/vnd.cncf.notary.signature
│   │       └── sha256:b3178e4515278364cab15ebff699996aac51b81d6a4aa1d7957b64c8de6331b3
│   ├── sha256:927aba099cbf5408bdf566de45e63bb0fa64a57a2822dc3a3e87c3c4d06ff2ff
│   │   └── application/vnd.cncf.notary.signature
│   │       └── sha256:b6aba6ee0dc194abe49848428740046741d96e9493054abf94c3f4455f78c7d3
│   └── sha256:c7d9a4272cd21fd69fd9878661417cb65b420c76cf3160bb275fd323329a1135
│       └── application/vnd.cncf.notary.signature
│           └── sha256:56444533031894671fb34a676c998fc72930f00156c0df639d48c970b41966df
├── application/vnd.cncf.notary.signature
│   └── sha256:d0ee1e9ae625fc5f2f0b279cf5c88ac69c760f6e0dc6cb9aa413e1e2a32ae539
└── application/spdx+json
    └── sha256:f869ea4870a14a697c1bbda5d7d59edc496838ff97b49d168f37a512759c3525
        └── application/vnd.cncf.notary.signature
            └── sha256:a1d71ce623a6ae71b068c4ee81b2cabaa368d53f2ae87ead042ac9b9d5aa7750
toddysm@tsm-mbp-msft ~
```

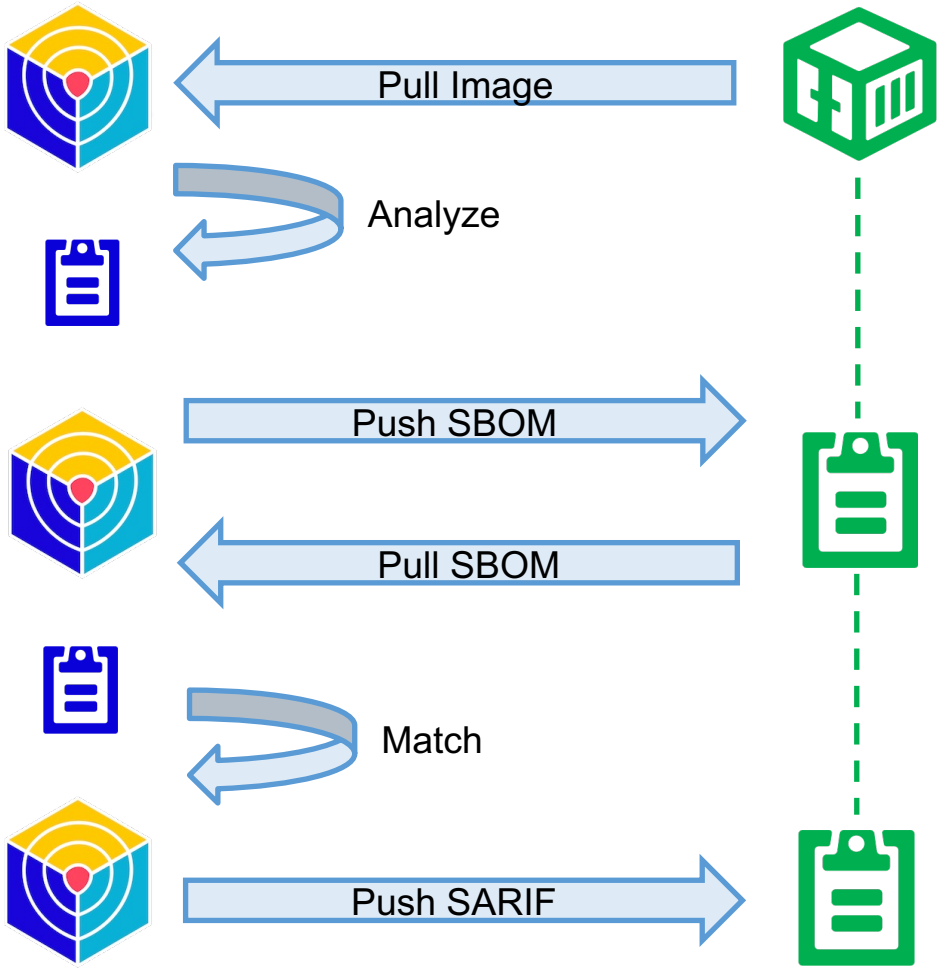
```
[ toddysm@tsm-mbp-msft ~ oras discover tsmacrusw3kubeconeu23.azurecr.io/kubeconeu23-python:3.11.2-slim --artifact-type application/sarif+json -o tree
[ toddysm@tsm-mbp-msft ~ oras discover tsmacrusw3kubeconeu23.azurecr.io/kubeconeu23-python@sha256:10a663cf824a11c0c7728afc45a036603400ca12a4cdde8a9d71701210981ce5 -o tree
tsmacrusw3kubeconeu23.azurecr.io/kubeconeu23-python@sha256:10a663cf824a11c0c7728afc45a036603400ca12a4cdde8a9d71701210981ce5
└── application/vnd.cncf.notary.signature
    └── sha256:b3178e4515278364cab15ebff699996aac51b81d6a4aa1d7957b64c8de6331b3
toddysm@tsm-mbp-msft ~
toddysm@tsm-mbp-msft ~
```

toddysm

Trivy & OCI



Trivy & OCI



Demo

KubeCon CloudNativeCon Europe 2023

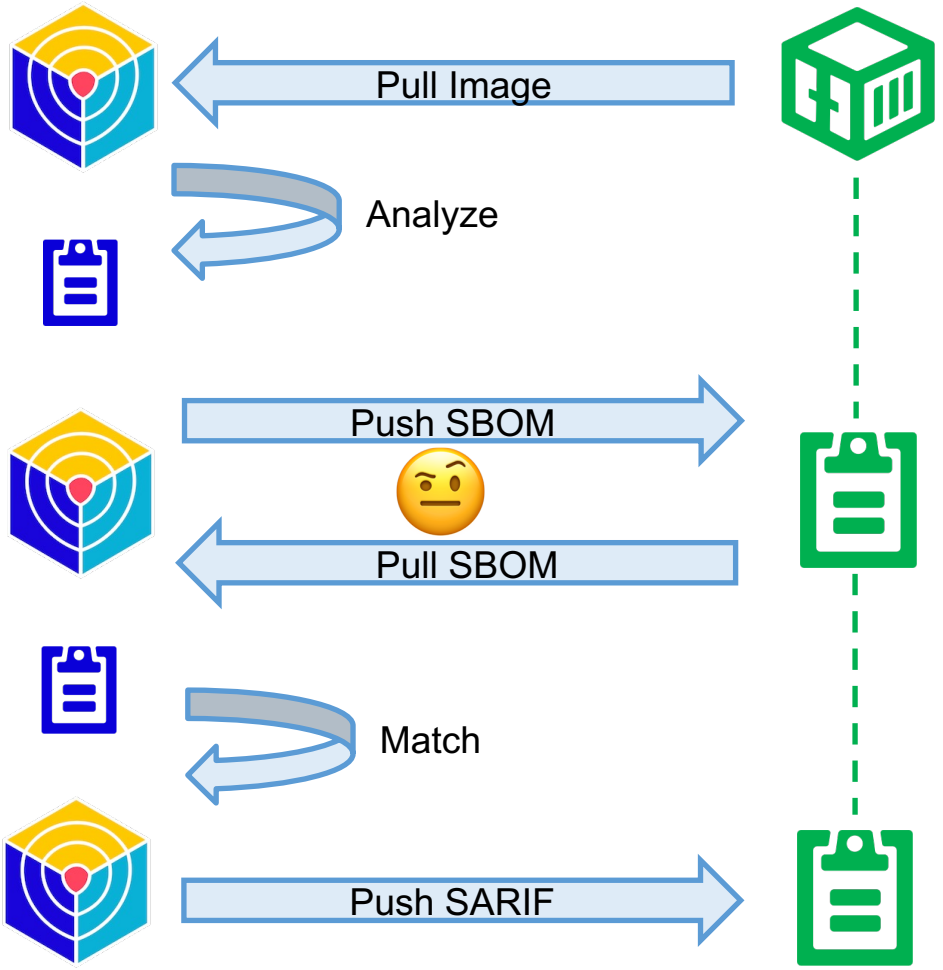
```
❯ ./trivy image localhost:5002/zot:latest --sbom-sources oci
2023-03-28T21:01:37.373+0300    INFO    Vulnerability scanning is enabled
2023-03-28T21:01:37.373+0300    INFO    Secret scanning is enabled
2023-03-28T21:01:37.373+0300    INFO    If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2023-03-28T21:01:37.373+0300    INFO    Please see also https://aquasecurity.github.io/trivy/dev/docs/secret/scanning/#recommendation for faste
2023-03-28T21:01:37.696+0300    INFO    Detected SBOM format: spdx-json
2023-03-28T21:01:37.757+0300    INFO    Found SBOM (spdx) in the OCI referrers
2023-03-28T21:01:37.762+0300    INFO    Detected OS: debian
2023-03-28T21:01:37.762+0300    INFO    Detecting Debian vulnerabilities...
2023-03-28T21:01:37.770+0300    INFO    Number of language-specific files: 1
2023-03-28T21:01:37.770+0300    INFO    Detecting gobinary vulnerabilities...

localhost:5002/zot:latest (debian 11.6)

Total: 13 (UNKNOWN: 0, LOW: 11, MEDIUM: 2, HIGH: 0, CRITICAL: 0)
```

Library	Vulnerability	Severity	Installed Version	Fixed Version	Title
libc6	CVE-2010-4756	LOW	2.31-13+deb11u5		glibc: glob implementation can cause excessive CPU and memory consumption due to... https://avd.aquasec.com/nvd/cve-2010-4756
	CVE-2018-20796				glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c https://avd.aquasec.com/nvd/cve-2018-20796
	CVE-2019-1010022				glibc: stack guard protection bypass https://avd.aquasec.com/nvd/cve-2019-1010022

Trusting the SBOM



Signing artifacts

sigstore cosign

notary

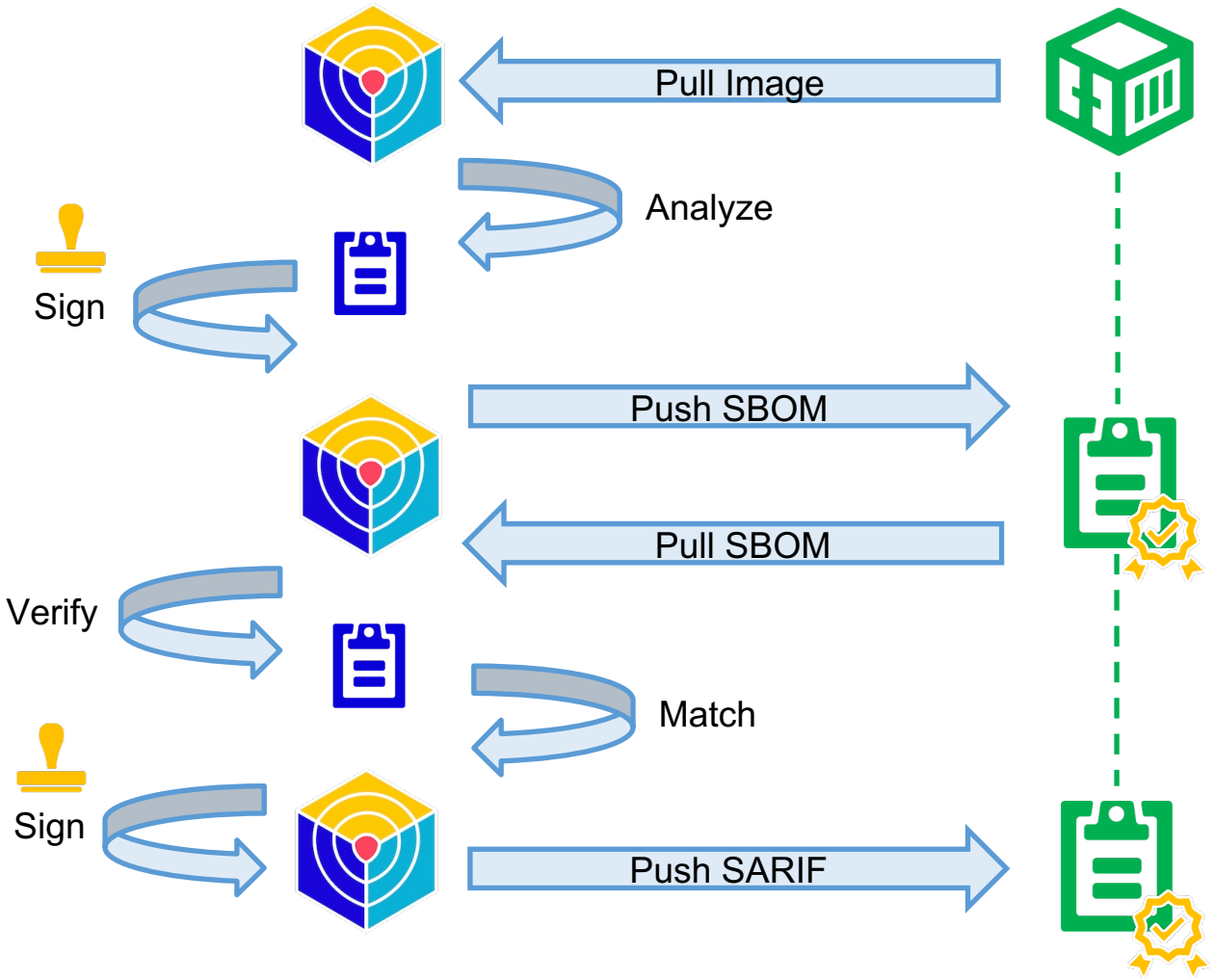
Demo

KubeCon CloudNativeCon Europe 2023

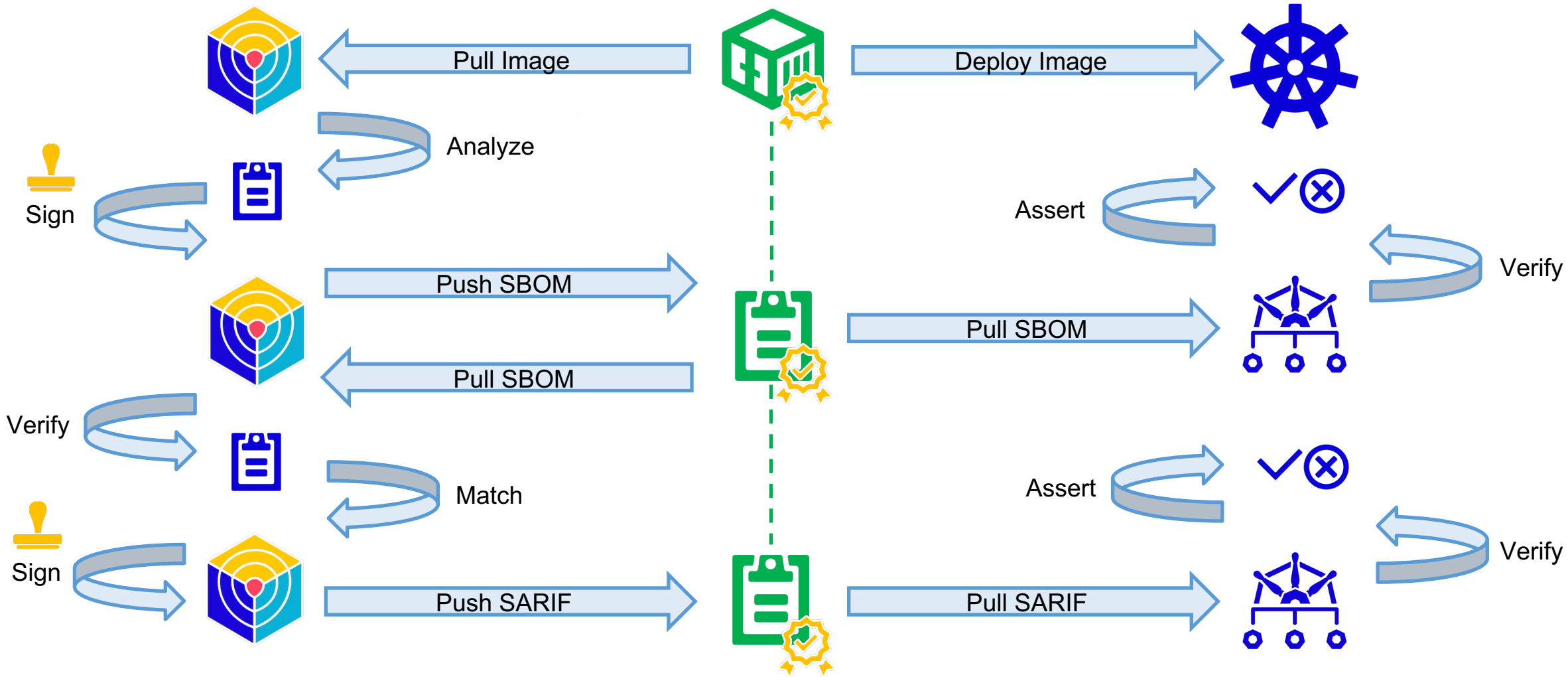
Development — /Users/toddysm/Documents/Development/cssc-pipeline/demos/kubecon-eu-2023/trivy-vuln-management/copy-and-resign.sh — copy-and-resign.sh — 170×40

```
$ regctl artifact tree $DEST_IMAGE
Ref: registry.twnt.co/flasksample06:kubeconeu-demo-v1
Digest: sha256:b4c0ed46d75ff7a1e8bcc166156db356dbb3768181d010a639ad4b4dd2f43db7
Referrers:
  - sha256:a4c385786f746946ca4d3171a4f820f7def4b928e09ddfc7171f9e30c3e4941b: application/spdx+json
    Referrers:
      - sha256:37f08e40f38bff3a1835420edacef3431a1c9a50efb265118f3f4ca1036fbd5c: application/vnd.dev.cosign.artifact.sig.v1+json
      - sha256:3307c0a3f6c2c82d4ec3fa0bd3b502fe8fa73def97573cd409e072a9babb8c2b: application/vnd.cncf.notary.signature
  - sha256:b37a4a1922a22a09163c7e09188360650e308d15668c8514bc2ce8ea547eb652: application/vnd.cyclonedx
    Referrers:
      - sha256:92d6e0a550de36f902703a054af732ea4f7c3f39b73ea80630acec004e863181: application/vnd.dev.cosign.artifact.sig.v1+json
      - sha256:bf418493f33003c4d1a242adce8274f30faa27f821e54089569f0b8c38960c6e: application/vnd.cncf.notary.signature
  - sha256:cc264d05b3314fe9ad90a3e2313f1a3ad2ea794b0ef620fb0f0d548e9d1eb797: application/vnd.dev.cosign.artifact.sig.v1+json
  - sha256:ee3d278529de57d8f0f8d6988d33f21cd7d1a0cadd79f9c6c128e26c33324f55: application/sarif+json
    Referrers:
      - sha256:c47a92b0c5e55f3eadf646db3a9310d6d5f0272cce60a78e67e8e49ed51842e8: application/vnd.dev.cosign.artifact.sig.v1+json
      - sha256:fa70e7525cfd440b84fefbca23a04ba3ebaa889383b38f13e9d5c266a327d9ec: application/vnd.cncf.notary.signature
  - sha256:9a691b6d16d534bb307db2378273753c7f3656ce019c29b16f130f975c914042: application/vnd.cncf.notary.signature
$
```

Signing artifacts



Demo


Pull Image
Deploy Image
Analyze
Sign
Assert
Verify
Push SBOM
Pull SBOM
Pull SBOM
Verify
Match
Assert
Sign
Verify
Push SARIF
Pull SARIF

Demo


```yaml
spec:
  validationFailureAction: Enforce
  webhookTimeoutSeconds: 30
  rules:
    - name: policy-vulnerabilities
      match:
        any:
        - resources:
            kinds:
              - Pod
      context:
      - name: keys
        configMap:
          name: keys
          namespace: kyverno
      verifyImages:
      - type: Notary
        imageReferences:
          - "registry.twnt.co/*"
        attestations:
          - predicateType: application/sarif+json
            attestors:
            - entries:
                - keys:
                    publicKeys: "{{ keys.data.notary }}"
              conditions:
                - all:
                  - key: "{{ runs[].tool.driver.rules[].properties.tags[] }}"
                    operator: AllNotIn
                    value: ["CRITICAL", "HIGH"]
```

```yaml
spec:
  validationFailureAction: Enforce
  webhookTimeoutSeconds: 30
  rules:
    - name: policy-licenses
      match:
        any:
        - resources:
            kinds:
              - Pod
      verifyImages:
      - type: Notary
        imageReferences:
          - "registry.twnt.co/*"
        attestations:
          - predicateType: application/vnd.cyclonedx
            attestors:
            - entries:
                - keys:
                    publicKeys: "{{ keys.data.notary }}"
              conditions:
                - all:
                  - key: "{{ bomFormat }}"
                    operator: Equals
                    value: "CycloneDX"
                  - key: "{{ time_since('','{{metadata.timestamp}}','') }}"
                    operator: LessThanOrEquals
                    value: "7d"
                  - key: "{{ components[].licenses[].expression }}"
                    operator: AllNotIn
                    value: ["GPL-2.0", "GPL-3.0"]
```

Lessons & Tips

- Artifact types can be inaccurate (or misleading).
  What kind of scan does a SARIF report represent?
- Annotations standardization
  `org.opencontainers.image.created`
  `org.opencontainers.image.vendor`
  `createdby=trivy`
- Getting specific artifact
  Sever-side: artifact type
  Client-side quick: annotations
  Client-side accurate: parse contents
  `` `trivy referrer get` ``
- Specifications
  Trivy SBOM vs Generic SBOM
  SARIF image metadata, summaries

itaysk
toddysm

KubeCon CloudNativeCon Europe 2023
North America 2021

Session Feedback

github.com/itaysk/kubeconeu23-oci-vuln

itaysk
toddysm