
KubeCon
CloudNativeCon
North America 2023


KubeCon | CloudNativeCon

North America 2023

What's New in Harbor, and How Can You Make Harbor Even Better

Yan Wang, VMWare
Vadim Bauer, 8gears

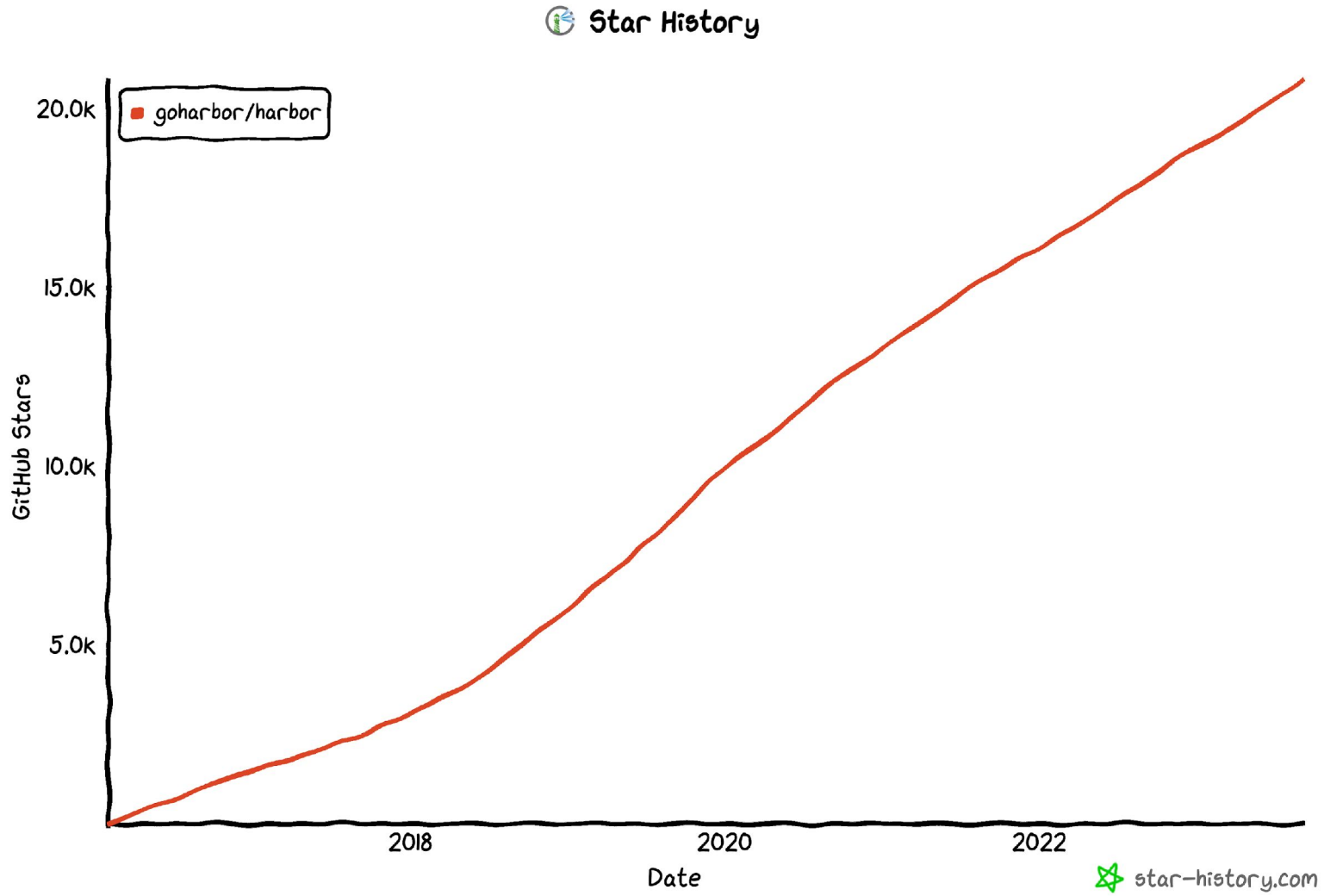
Agenda

- Introduction
- Harbor Superpowers
- Feature Recap
  - Security Hub
  - OCI Distribution Spec v1.1
  - Robot Full Access
  - Other Enhancements
- Demo
- Future Outlook
- Collaboration and how to make Harbor better

Introduction

Harbor is a CNCF-graduated open-source container registry to store and manage container images and other OCI artifacts securely with policies, role-based access control, vulnerability analytics and signing.

Introduction

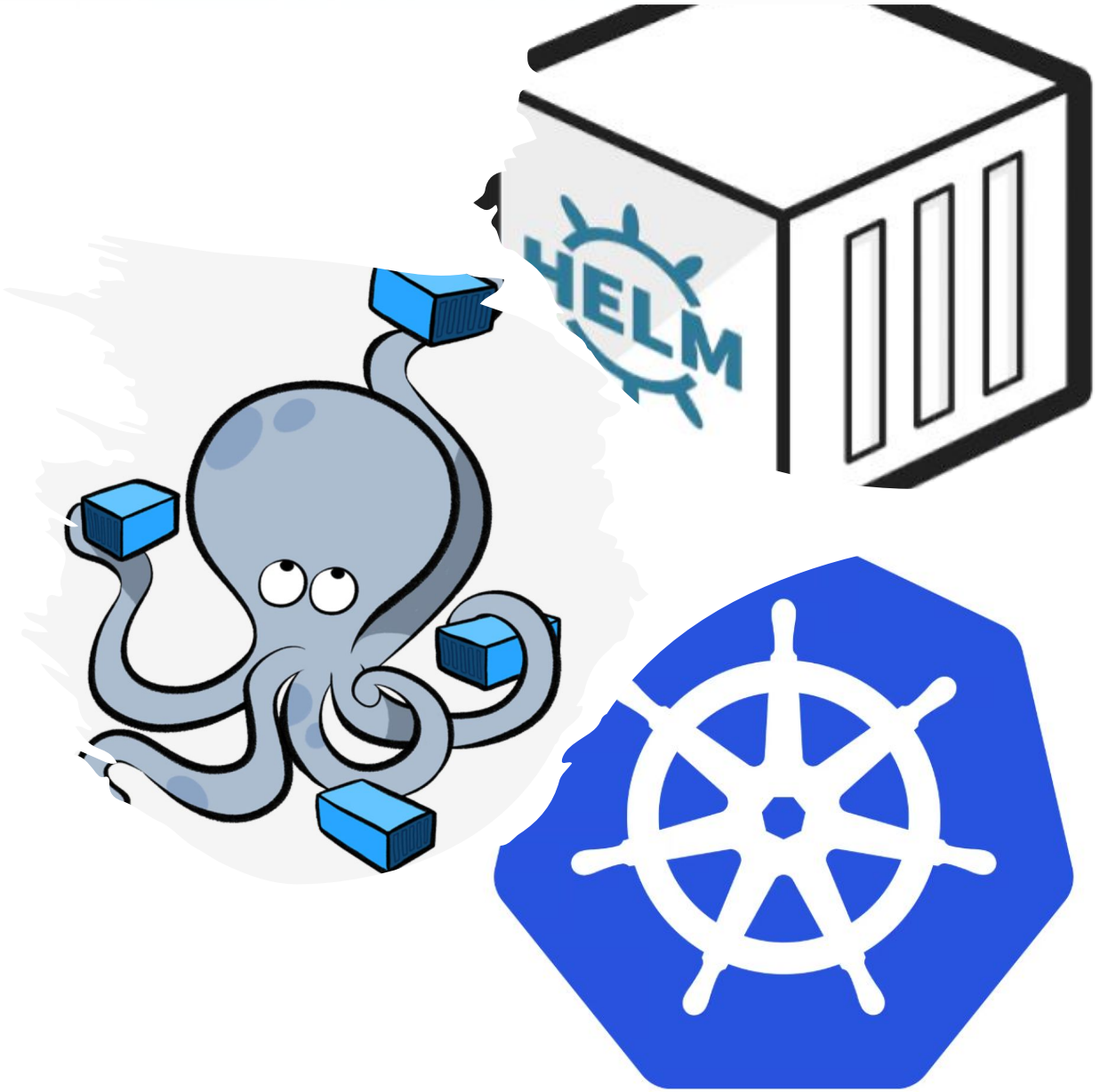


“Harbor is the golden standard when it comes to container registries.”

Victor Farcic

Key Features

- Access Control
  - RBAC, Project Isolation
- Artifact Distribution
  - Replication, Proxy Cache, P2P Preheat
- Security & Compliance
  - Vulnerability Scan, Artifact Signature, CVE Export, Security Hub
- Policy & Maintainability
  - Quota, Immutability, Retention, Garbage Collection, Log Rotation
- Extensibility
  - OIDC/LDAP Authentication, Webhook, Pluggable Scanner, Robot Account



Superpowers

1. **Works for small Teams and Enterprises**
    a. RBAC
    b. IDP and SSO - External identity provider for **authentication** and **authorization**
2. **Makes CISOs happy**
    a. All your images in one place – Replication, Proxying
    b. Vulnerability overview, audit trails
3. **Ops people's darling**
    a. Automation & IaC – RESTful API, Terraform, Pulumi
    b. Operational control mechanisms – GC, Quota, Polices

Superpowers

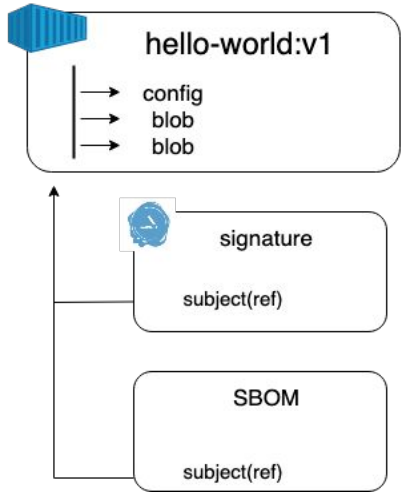
Let me show that …

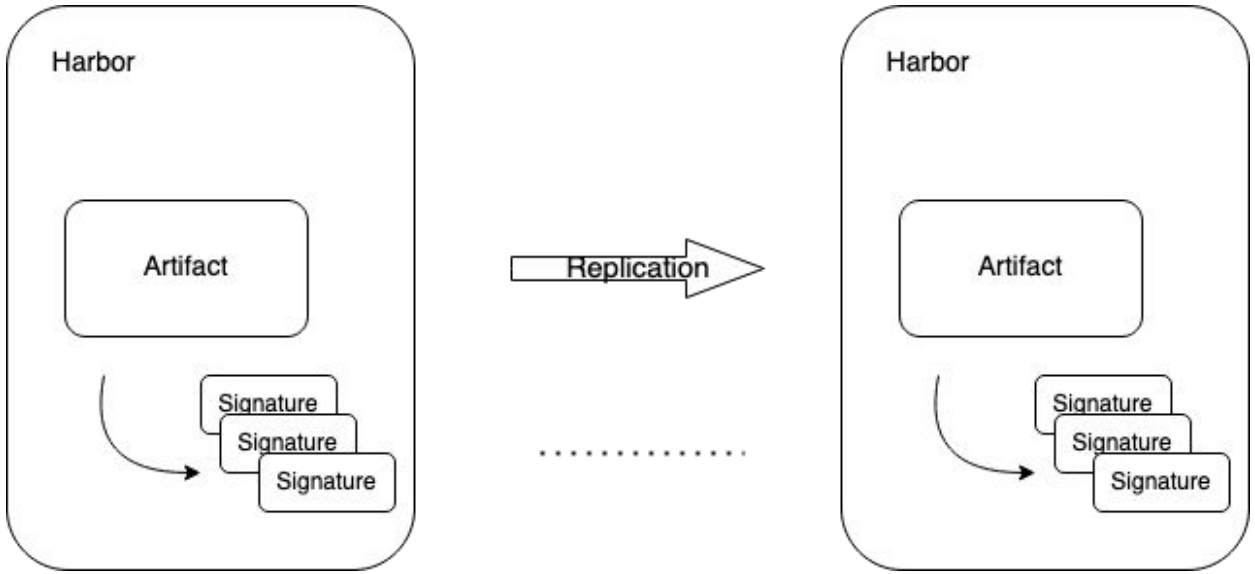
Architecture

OCI

OCI Distribution Spec v1.1.0-rc3

- Establish connections between artifacts by utilizing the subject attribute.
- Enable the storage of Notation signatures and Nydus conversions as referrers.
- Successfully implemented the Referrers API.

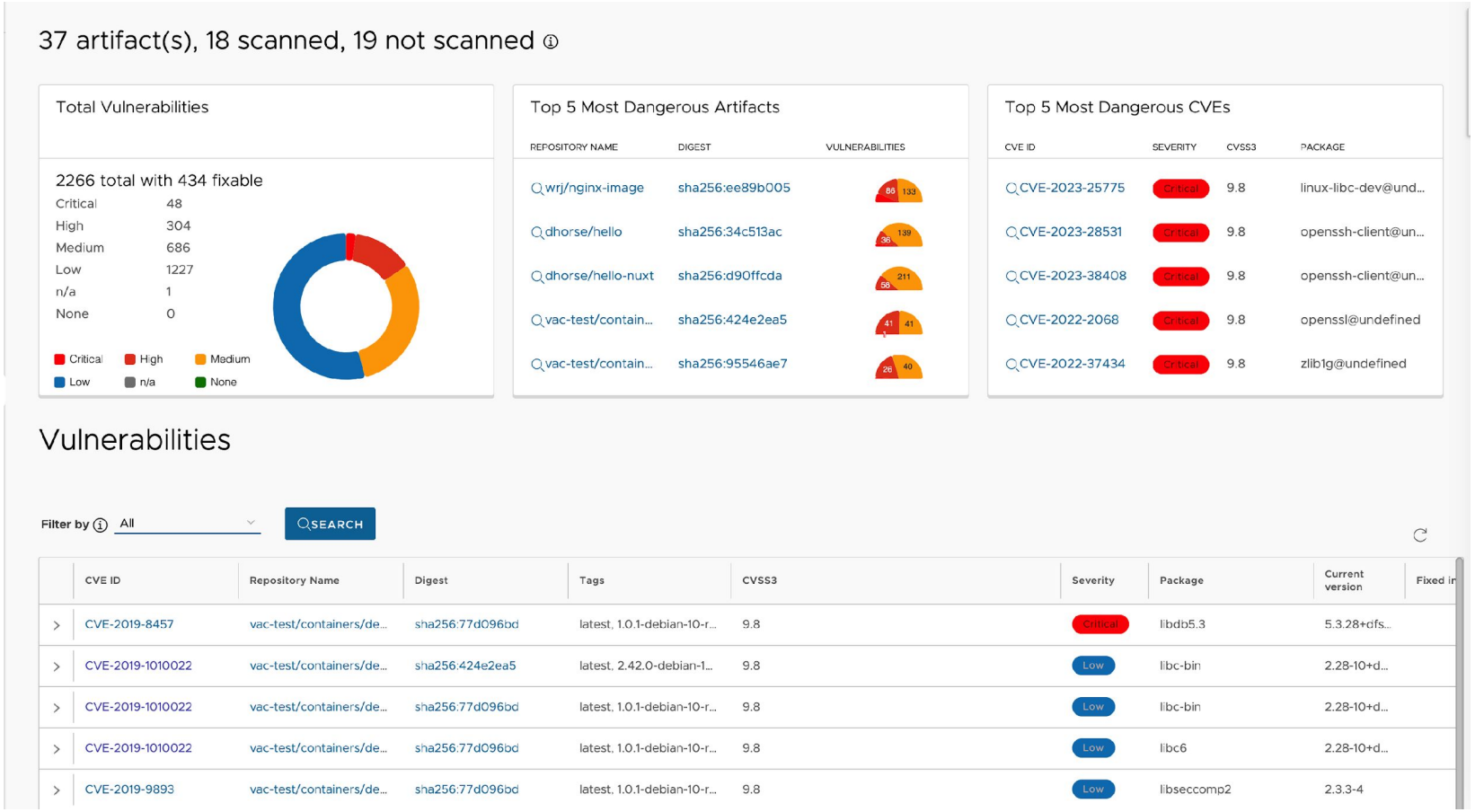




Demo -- OCI

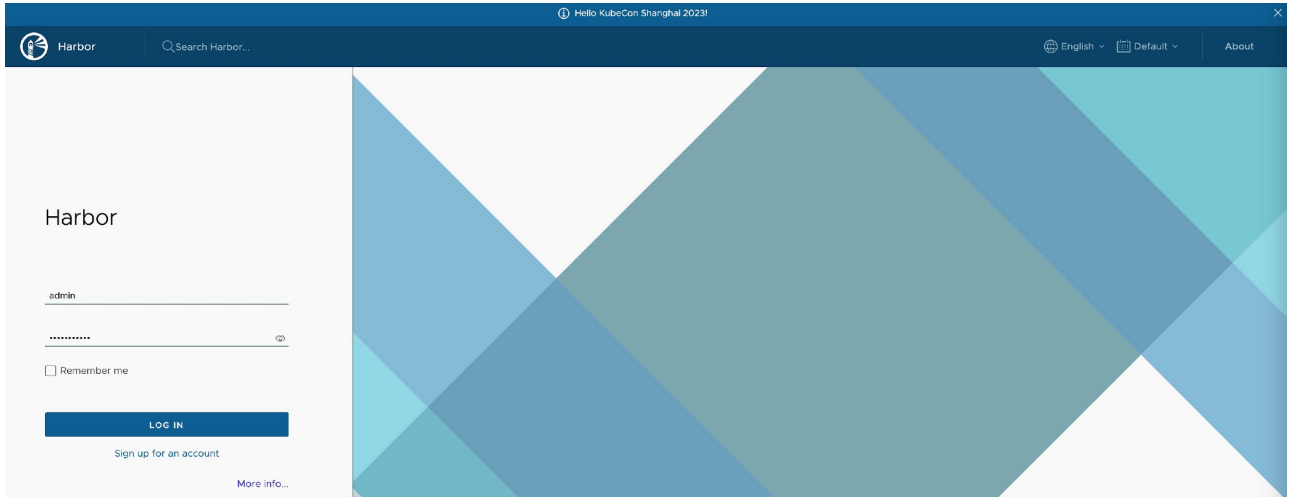
Security Hub

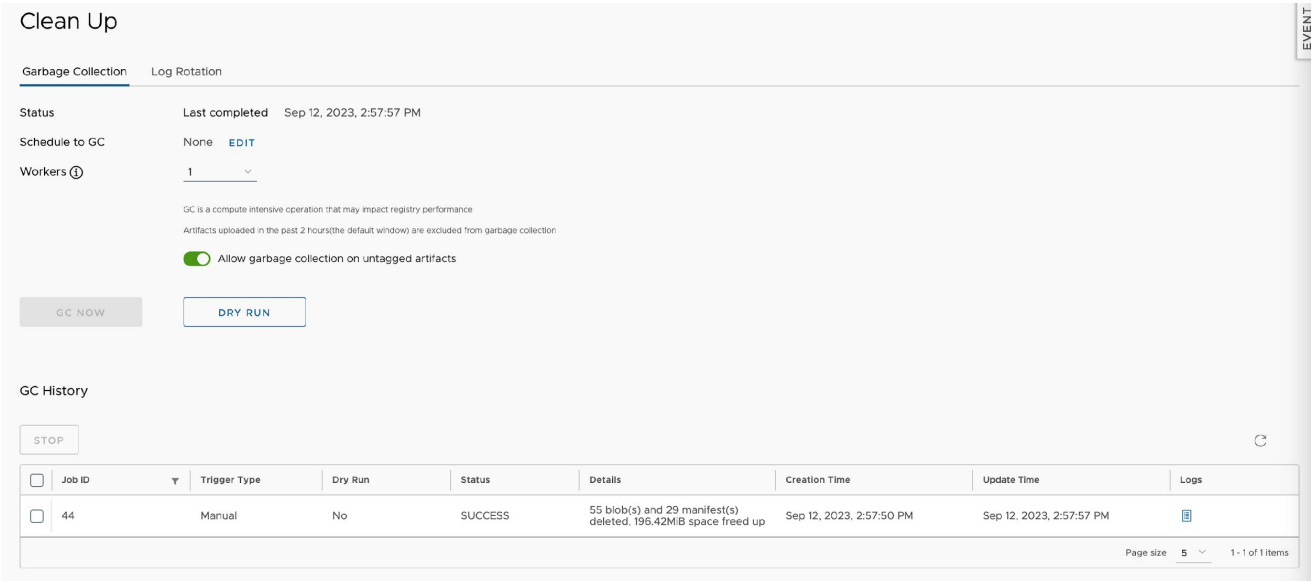
- Offer a comprehensive and centralized overview of the current security status of artifacts stored in Harbor.
- Emphasize the identification of the most critical artifacts and CVEs.
- Enable vulnerability search by attributes, including CVE ID, severity, project, repository, digest, and more.



Enhancements

- Introduce a customizable message banner to deliver comprehensive and detailed information about upcoming maintenance or admin activities.
- Enhance visibility by providing a detailed GC execution history and enabling parallel deletion for quicker GC duration.
- Implement a new mechanism that utilizes Redis to optimize quota locks during high-concurrency pushes to the same project.

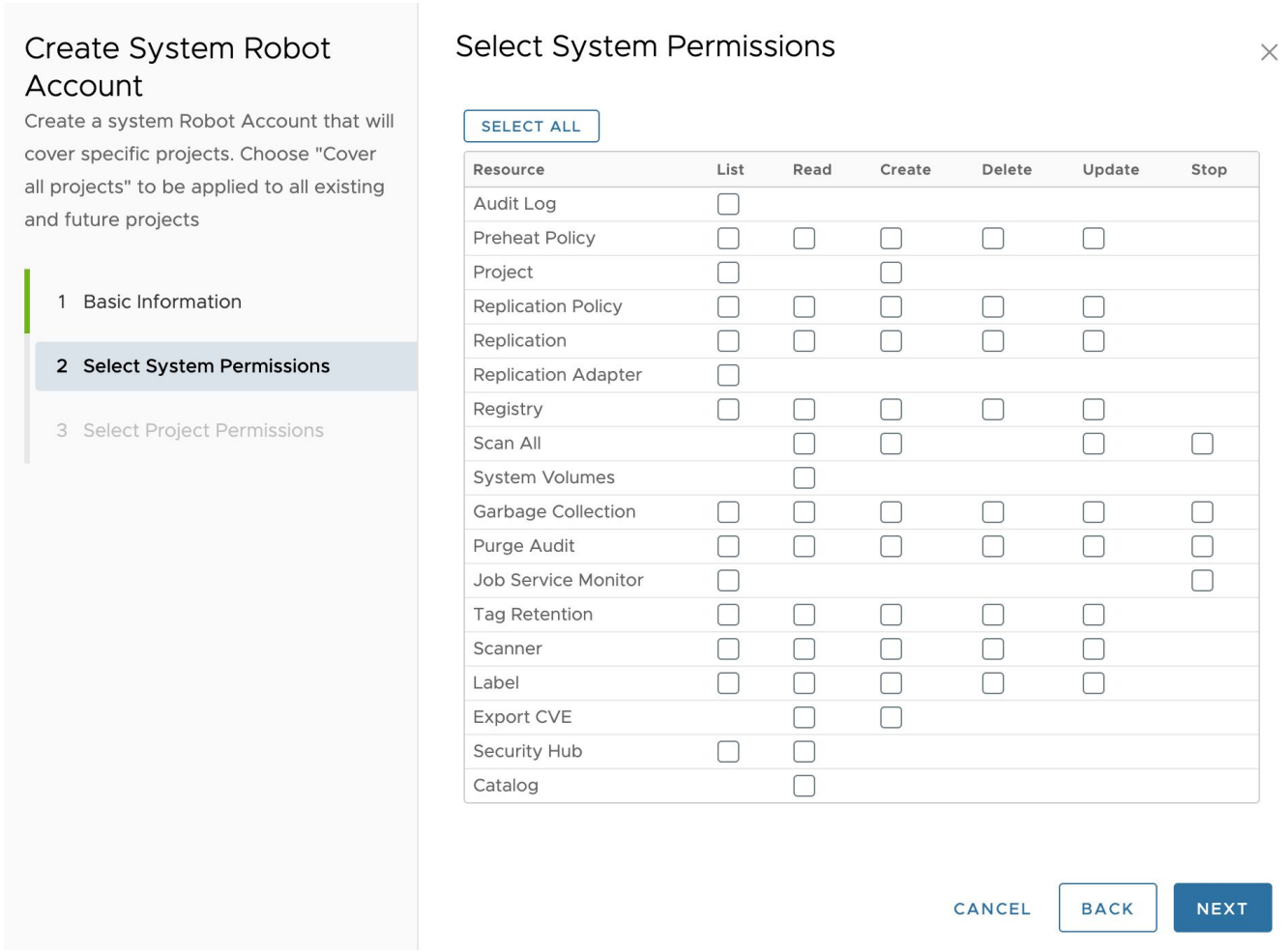




Demo

Robot Accounts – Full Access

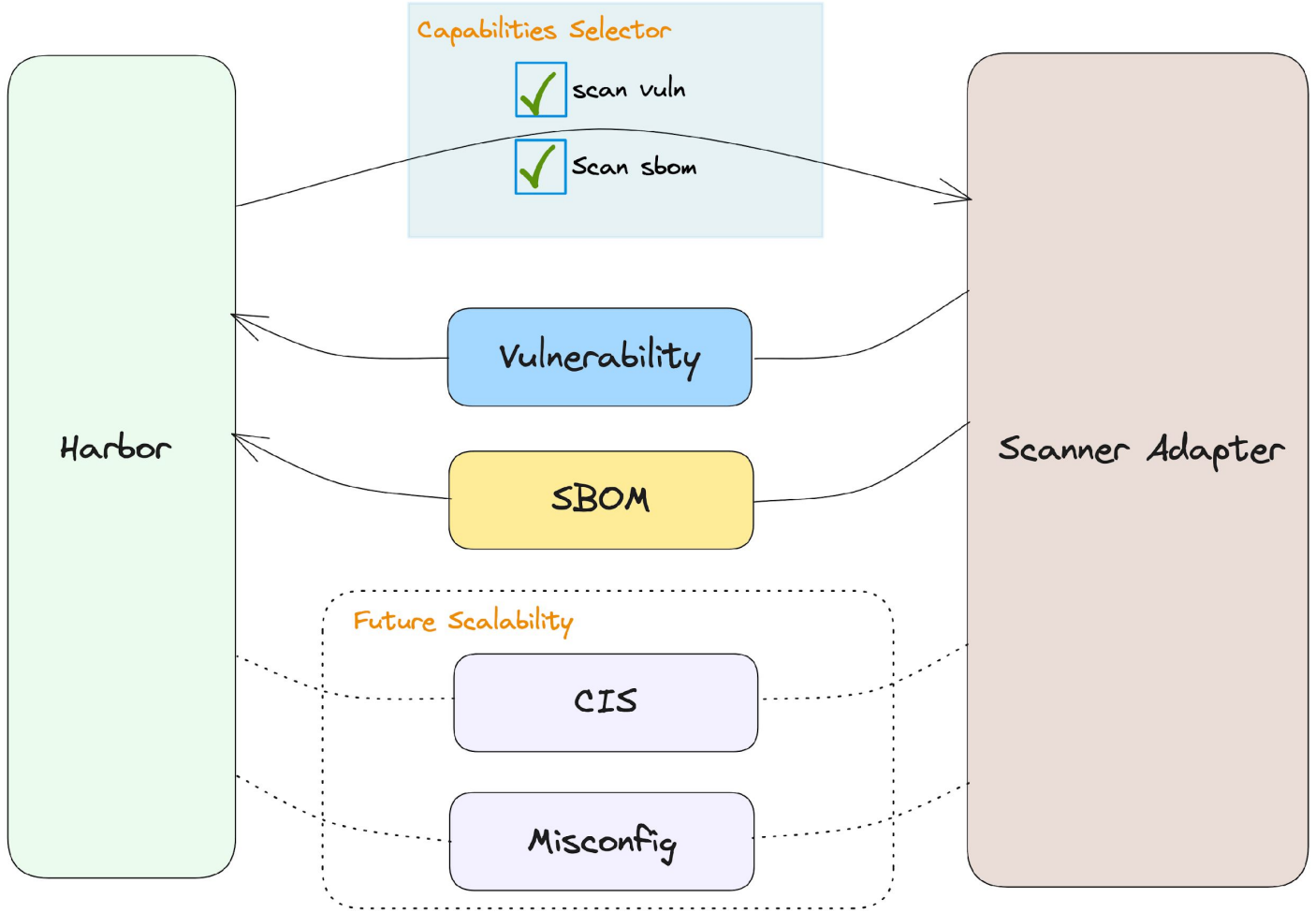
- Provides step-by-step instructions for attaching a robot account to a set of APIs, ensuring clear and straightforward.
- A user-friendly UI that displays the data dictionary, enabling users to make informed choices with ease.



Demo – Robot Accounts Full Access

Pluggable Scanner Spec – v1.2

- Enhance the scanner's capabilities and the scan request model to enable the specification of enabled capabilities for Harbor scanning.
- Introduce a new data report model for the Software Bill of Materials (SBOM) and outline the specifications during integration with Harbor.
- This new model will provide greater flexibility and convenience for future expansion of security scanning types, such as CIS and misconfig.
- Update the OpenAPI definitions YAML to version 1.2.



Pluggable Scanner Spec -- Metadata

application/vnd.scanner.adapter.metadata+json; version=1.0

0 removals 18 lines Copy

```
{
  "scanner": {
    "name": "Trivy",
    "vendor": "Aqua Security",
    "version": "0.4.0"
  },
  "capabilities": [
    {
      "consumes_mime_types": [
        "application/vnd.oci.image.manifest.v1+json",
        "application/vnd.docker.distribution.manifest.v2+json"
      ],
      "produces_mime_types": [
        "application/vnd.scanner.adapter.vuln.report.harbor+json; version=1.0"
      ]
    }
  ]
}
```

application/vnd.scanner.adapter.metadata+json; version=1.1

11 additions 29 lines Copy

```
{
  "scanner": {
    "name": "Trivy",
    "vendor": "Aqua Security",
    "version": "0.4.0"
  },
  "capabilities": [
    {
      "type": "vulnerability",
      "consumes_mime_types": [
        "application/vnd.oci.image.manifest.v1+json",
        "application/vnd.docker.distribution.manifest.v2+json"
      ],
      "produces_mime_types": [
        "application/vnd.scanner.adapter.vuln.report.harbor+json; version=1.0"
      ]
    },
    {
      "type": "sbom",
      "consumes_mime_types": [
        "application/vnd.oci.image.manifest.v1+json",
        "application/vnd.docker.distribution.manifest.v2+json"
      ],
      "produces_mime_types": [
        "application/vnd.security.sbom.report+json; version=1.0"
      ]
    }
  ]
}
```

Pluggable Scanner Spec -- Scan Request

application/vnd.scanner.adapter.scan.request+json; version=1.0

1 removal — 12 lines — Copy

```
{
  "registry": {
    "url": "https://core.harbor.domain",
    "authorization": "Basic BASE64_ENCODED_CREDENTIALS"
  },
  "artifact": {
    "repository": "library/mongo",
    "digest": "sha256:6c3c624b58dbbcd3c0dd82b4c53f04194d1247c6eebdaab7c610cf7d66709b3b",
    "tag": "3.14-xenial",
    "mime_type": "application/vnd.docker.distribution.manifest.v2+json"
  }
}
```

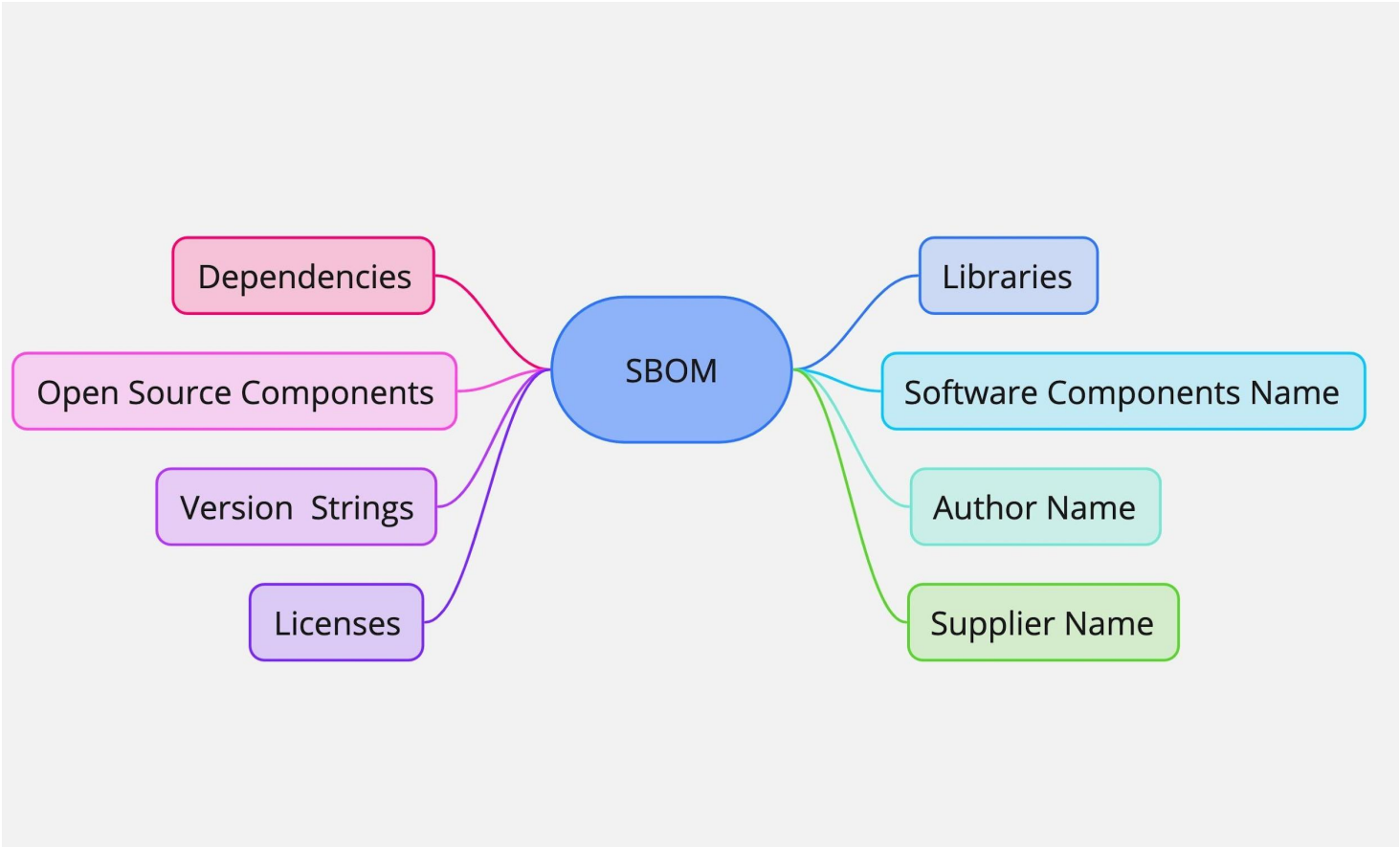
application/vnd.scanner.adapter.scan.request+json; version=1.1

15 additions — 26 lines — Copy

```
{
  "registry": {
    "url": "https://core.harbor.domain",
    "authorization": "Basic BASE64_ENCODED_CREDENTIALS"
  },
  "artifact": {
    "repository": "library/mongo",
    "digest": "sha256:6c3c624b58dbbcd3c0dd82b4c53f04194d1247c6eebdaab7c610cf7d66709b3b",
    "tag": "3.14-xenial",
    "mime_type": "application/vnd.docker.distribution.manifest.v2+json"
  },
  "enabled_capabilities": [
    {
      "type": "vulnerability"
    },
    {
      "type": "sbom",
      "produces_mime_types": [
        "application/vnd.security.sbom.report+json; version=1.0"
      ],
      "parameters": {
        "accept_media_type": "application/spdx+json"
      }
    }
  ]
}
```

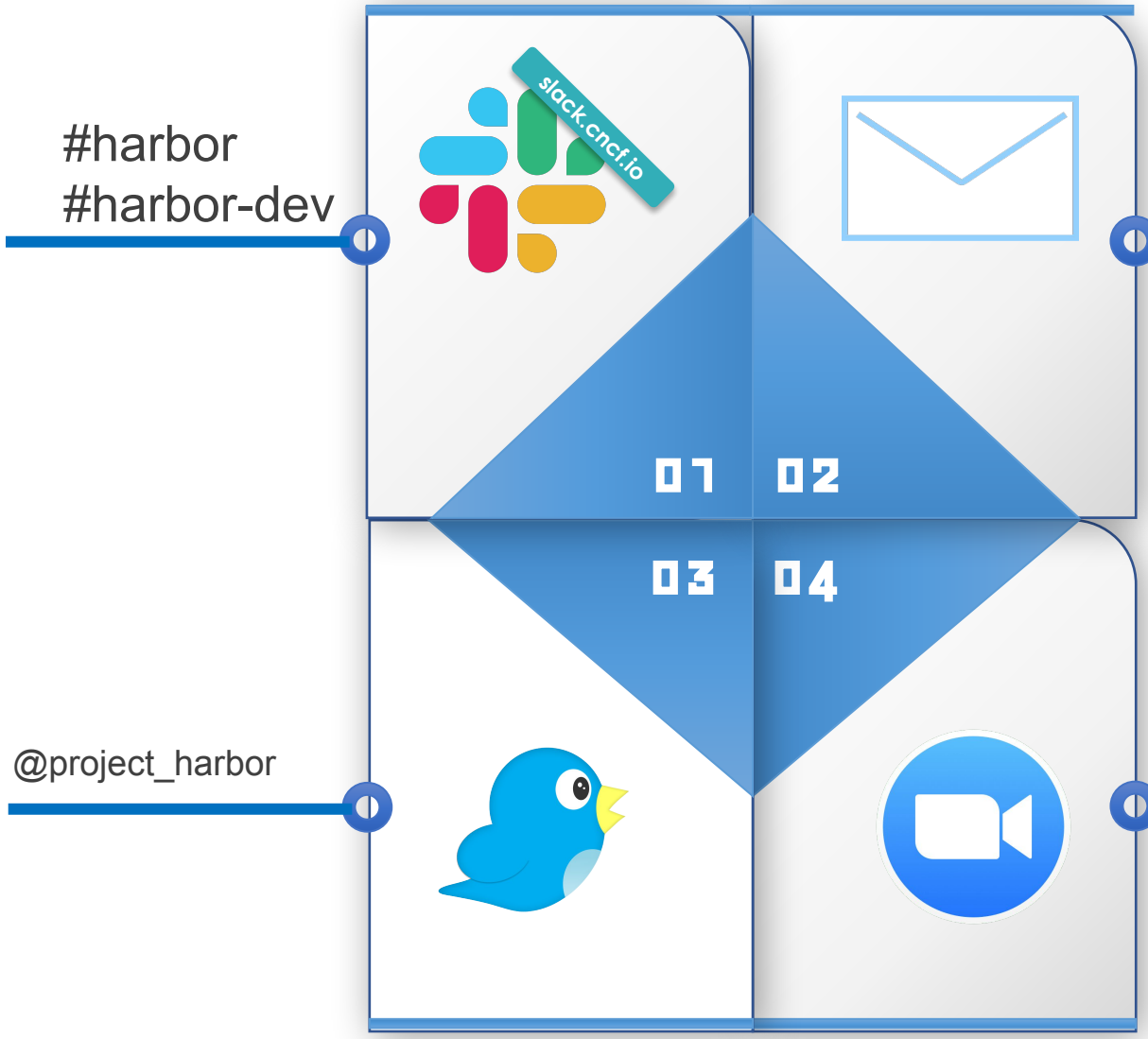
Software Bill of Materials

- Automatically generate SBOMs for OCI Artifacts.
- Accelerate the vulnerabilities scan of artifacts by utilizing SBOMs.
- Enable visual management and analysis of SBOMs, including features like export, download, and viewing.
- Integration with Security Hub offers a comprehensive global security overview.



Collaboration

#harbor
#harbor-dev



harbor-users@lists.cncf.io
harbor-dev@lists.cncf.io

@project_harbor

https://github.com/goharbor/community/wiki/Harbor-Community-Meetings

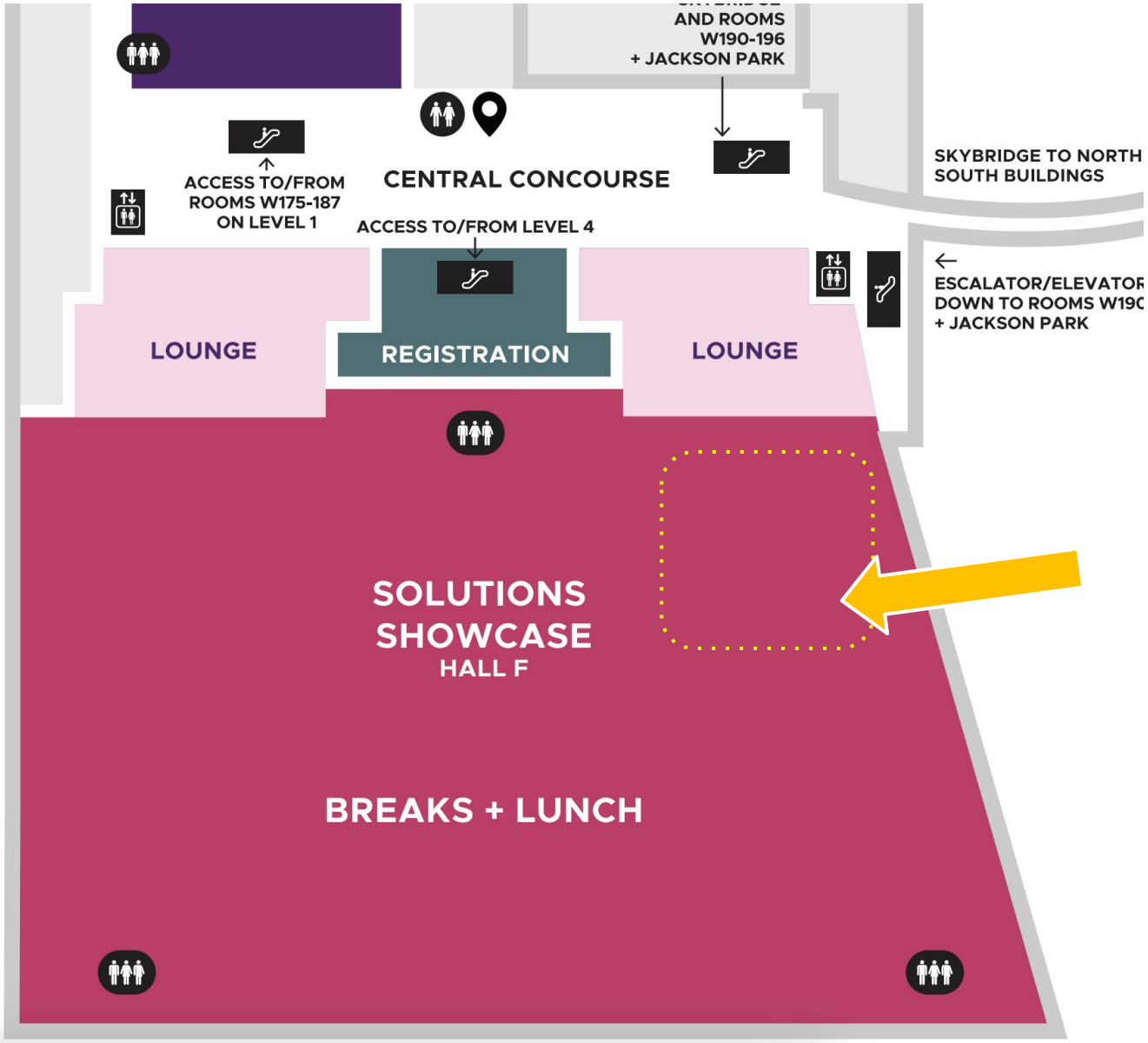
Meet The Team @ Project Kiosk

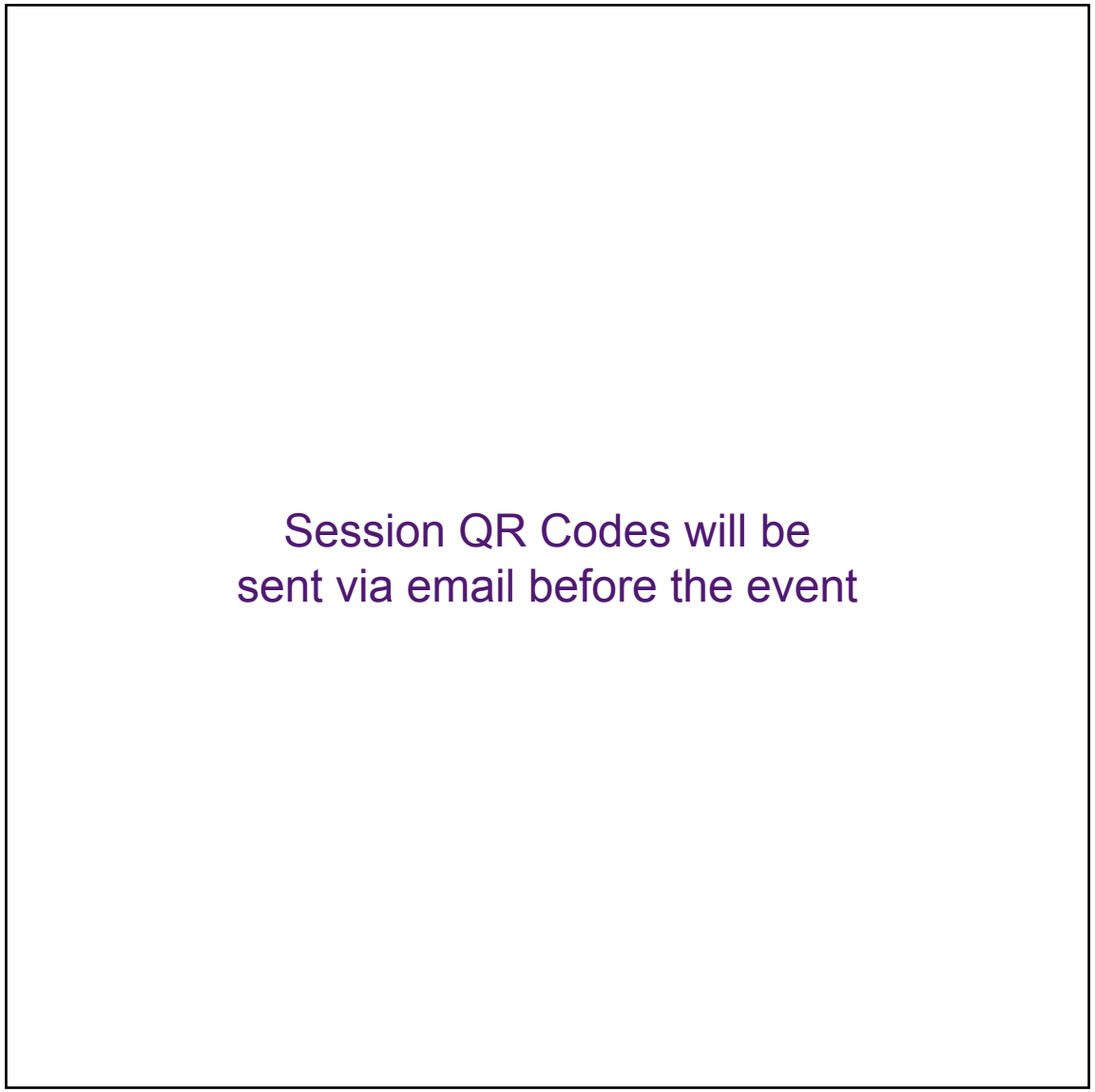
KubeCon CloudNativeCon North America 2023

CNCF Project Booth **P2**

Wednesday, **2:00 pm – 5:00 pm**

Thursday, **12:30 pm – 2:30 pm**





**Please scan the QR Code above
to leave feedback on this session**