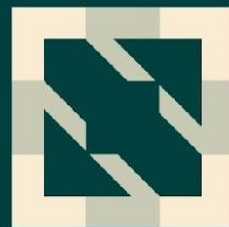




**KubeCon**



**CloudNativeCon**



**OPEN SOURCE SUMMIT**

**China 2023**



KubeCon



CloudNativeCon



OPEN SOURCE SUMMIT

China 2023

# Kicking Security Chain Attacks to the Curb with Kyverno and Notation in GitOps

**Shuting Zhao**, Staff Engineer, Nirmata

**Feynman Zhou**, Product Manager, Microsoft

# About us

- Staff Engineer at Nirmata
- Kyverno Co-creator and Maintainer
- Microsoft Product Manager
- Notary Project and ORAS maintainer



Shuting Zhao



@FeynmanZhou





# Agenda

- Concepts and Challenges of Software Supply Chain Security
- Recent Supply Chain Attack incidents
- Popular OSS solutions and framework in the industry and CNCF
- How Notation and Kyverno help secure software supply chain
- End-to-end demo: Signing and verify images on Kubernetes with GitOps



KubeCon



CloudNativeCon



OPEN SOURCE SUMMIT

China 2023

# Concepts and challenges of Software Supply Chain Security

# Traditional supply chain v.s. Software supply chain

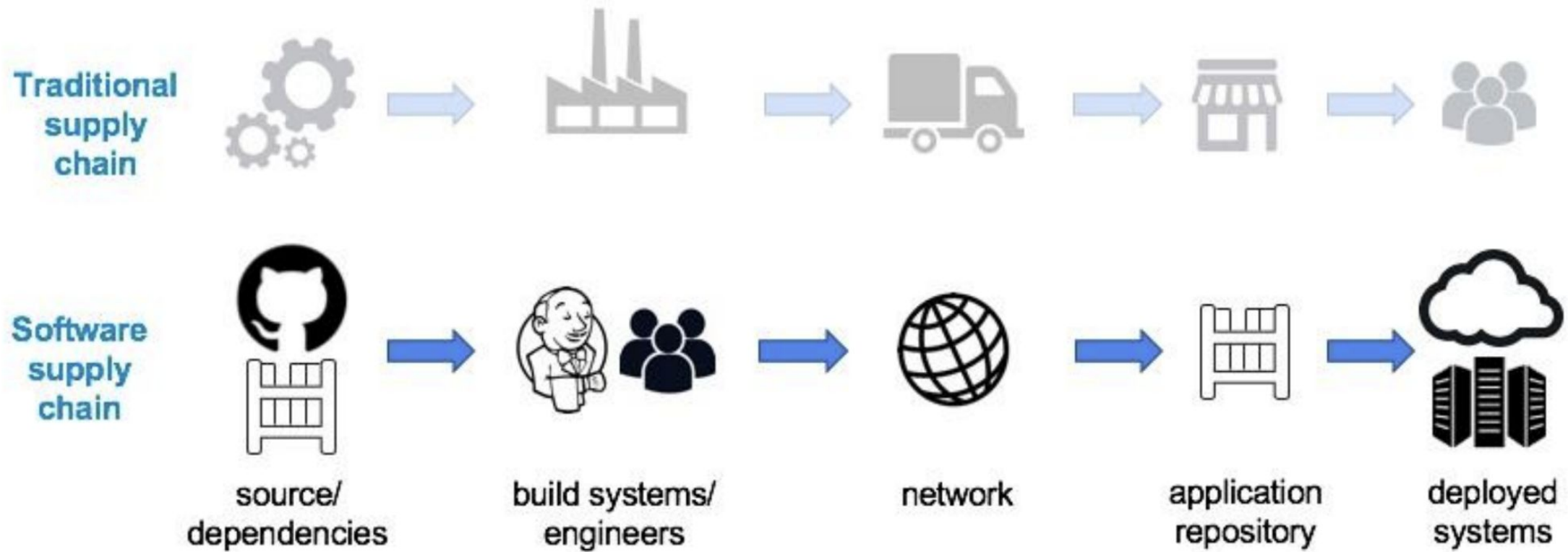
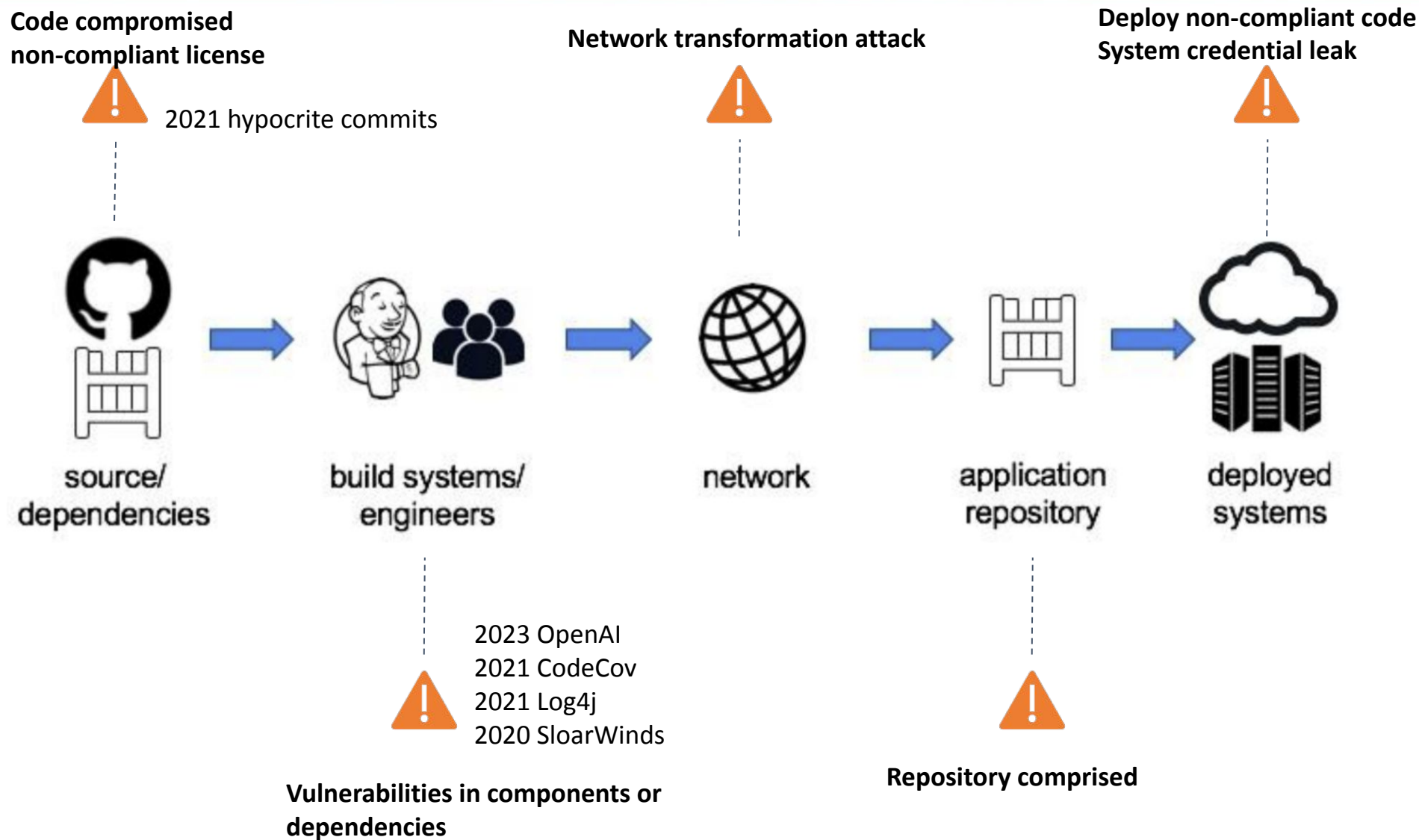


Image source: [CNCF Software Supply Chain Security Paper](#)

# Potential security attacks and incidents





From [《Synosys Open Source Security and Risk Analysis report - 2023》](#):

Of the **1,703** codebases scanned in 2022, **87%** included security and operational risk assessments.

**54%**

of codebases had  
license conflicts

**89%**

of codebases contained  
open source more than  
four years out-of-date

**31%**

of codebases  
contained open source  
with no license or a  
custom license

**91%**

of codebases contained  
components that had  
no new development in  
the past two years

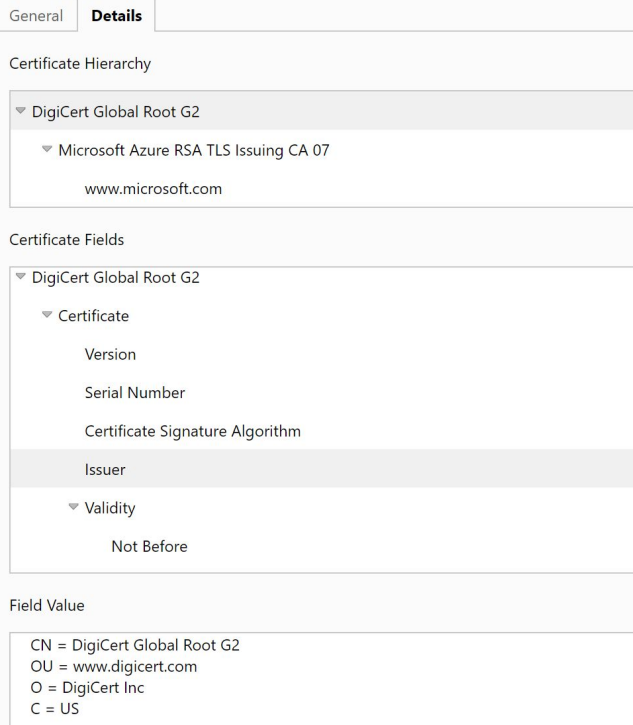


# Improve security posture in the digital world

## How SSL Certificate secures the website?



Certificate Viewer: www.microsoft.com



## Compare it with today's cloud-native application

- ✓ ghcr.io/kubecon/sample-image:signed
  - ✓ Signature
  - ✓ SBOM
  - ✓ Vulnerability scanning report
  - ✓ Provenance attestation
  - ✓ Image lifecycle metadata



KubeCon



CloudNativeCon



OPEN SOURCE SUMMIT

China 2023

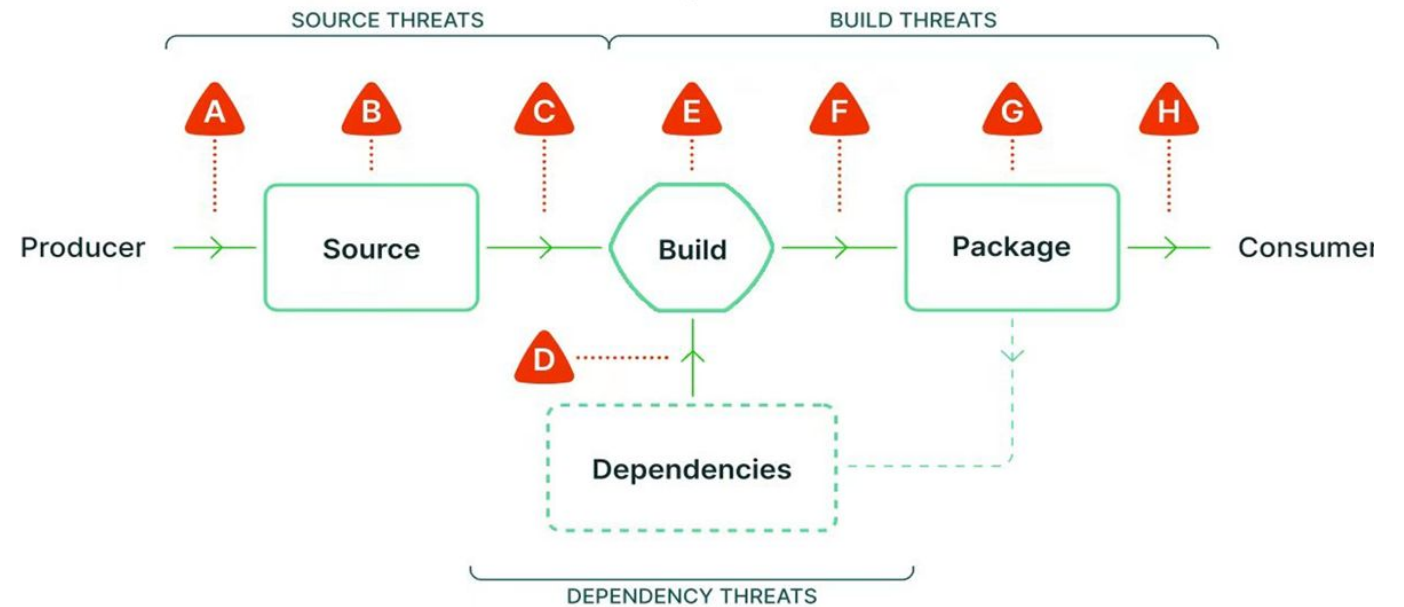
# Popular OSS solutions and frameworks in the Industry and CNCF

# Popular Supply Chain Security frameworks

Secure Supply Chain Consumption Framework (S2C2F)



SLSA framework





# Flourish security ecosystem in CNCF

## Security & Compliance



# Popular OSS projects for secure supply chain

- **Sign and verify OCI Image**

- Notation (Notary Project)
- Cosign

- **OCI Artifact distribution**

- ORAS
- Regctl
- Skopeo
- Crane

- **Generate SBOM**

- Microsoft sbom-tool
- Syft / Docker SBOM
- Xeol

- **Provenance attestation**

- in-toto attestation

- **Policy Management**

- Kyverno
- Open Policy Agent (OPA) gatekeeper

- **Admission controller**

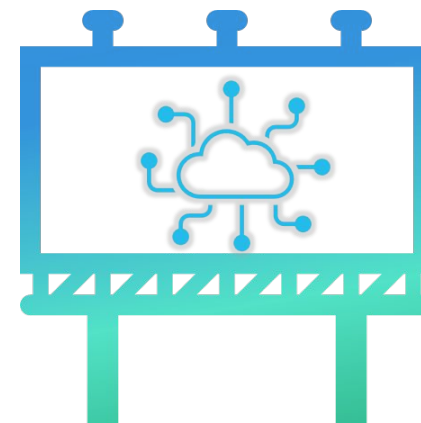
- Ratify, Connaisseur

- **Runtime security**

- Falco

- **Vulnerability scanning**

- Trivy
- Synk
- Clair





KubeCon



CloudNativeCon



OPEN SOURCE SUMMIT

China 2023

# How Notation and Kyverno help secure Software Supply Chain

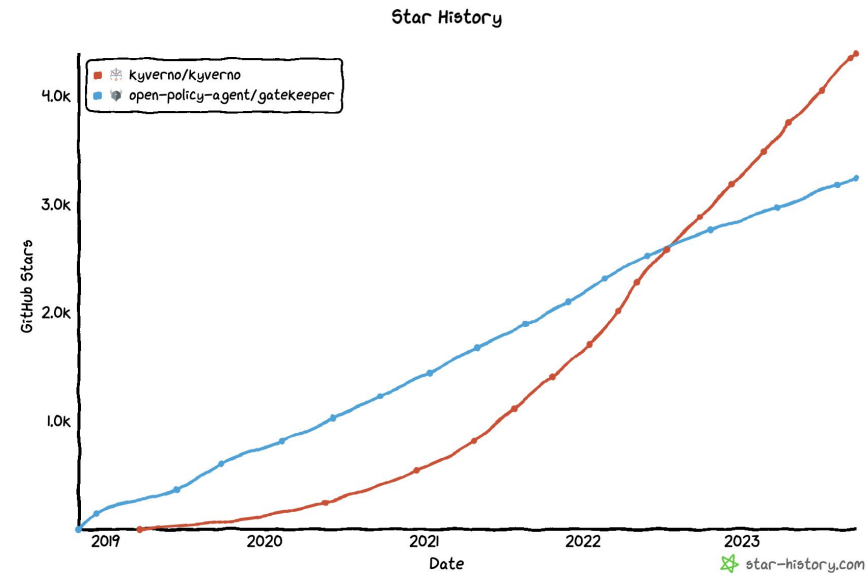


# What is Kyverno

## Kubernetes native policy engine



- 2.4 Billion+ image pulls
- 4.4K+ GitHub Stars
- 330+ contributors
- 2300+ Slack members
- 290+ policies



# What is Kyverno

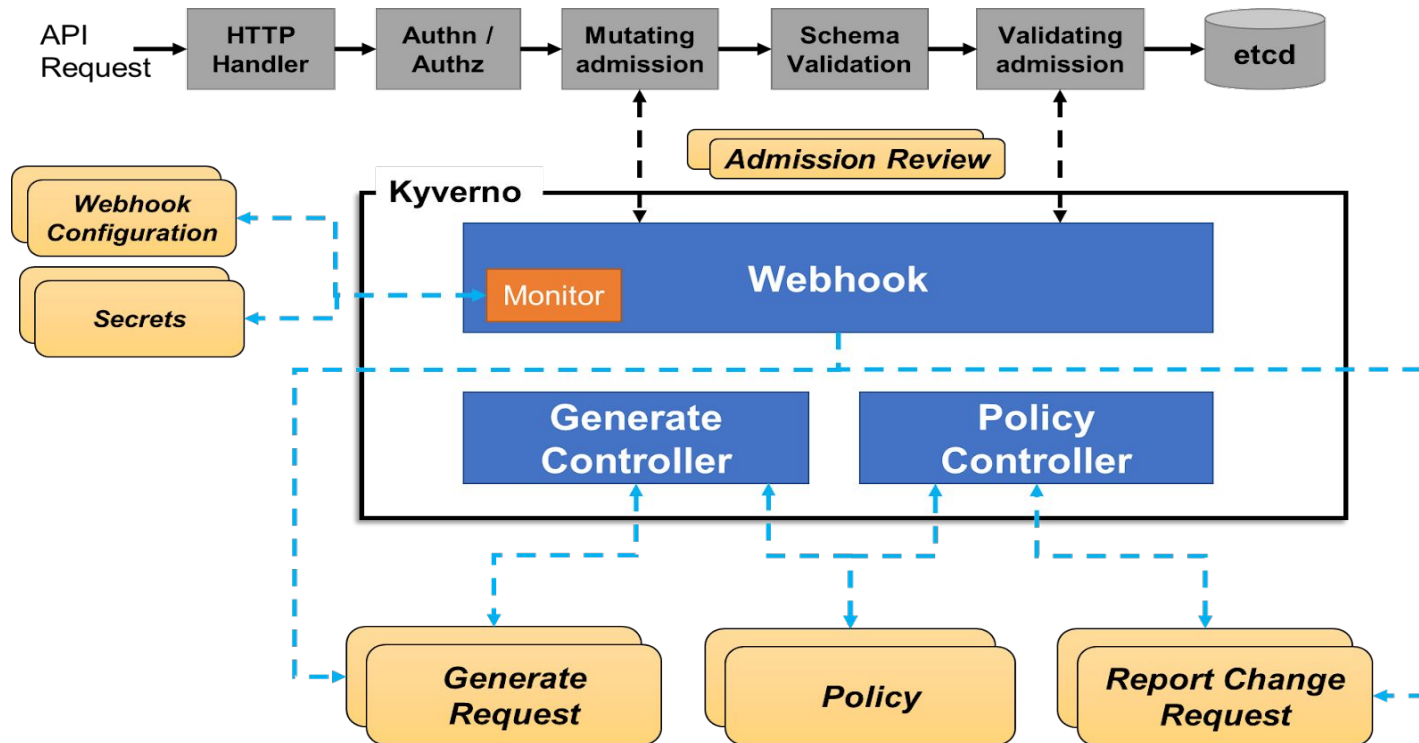
## Kubernetes native policy engine



- ❑ Eliminate misconfigurations
- ❑ Prevent vs. detect
- ❑ Shift-left security



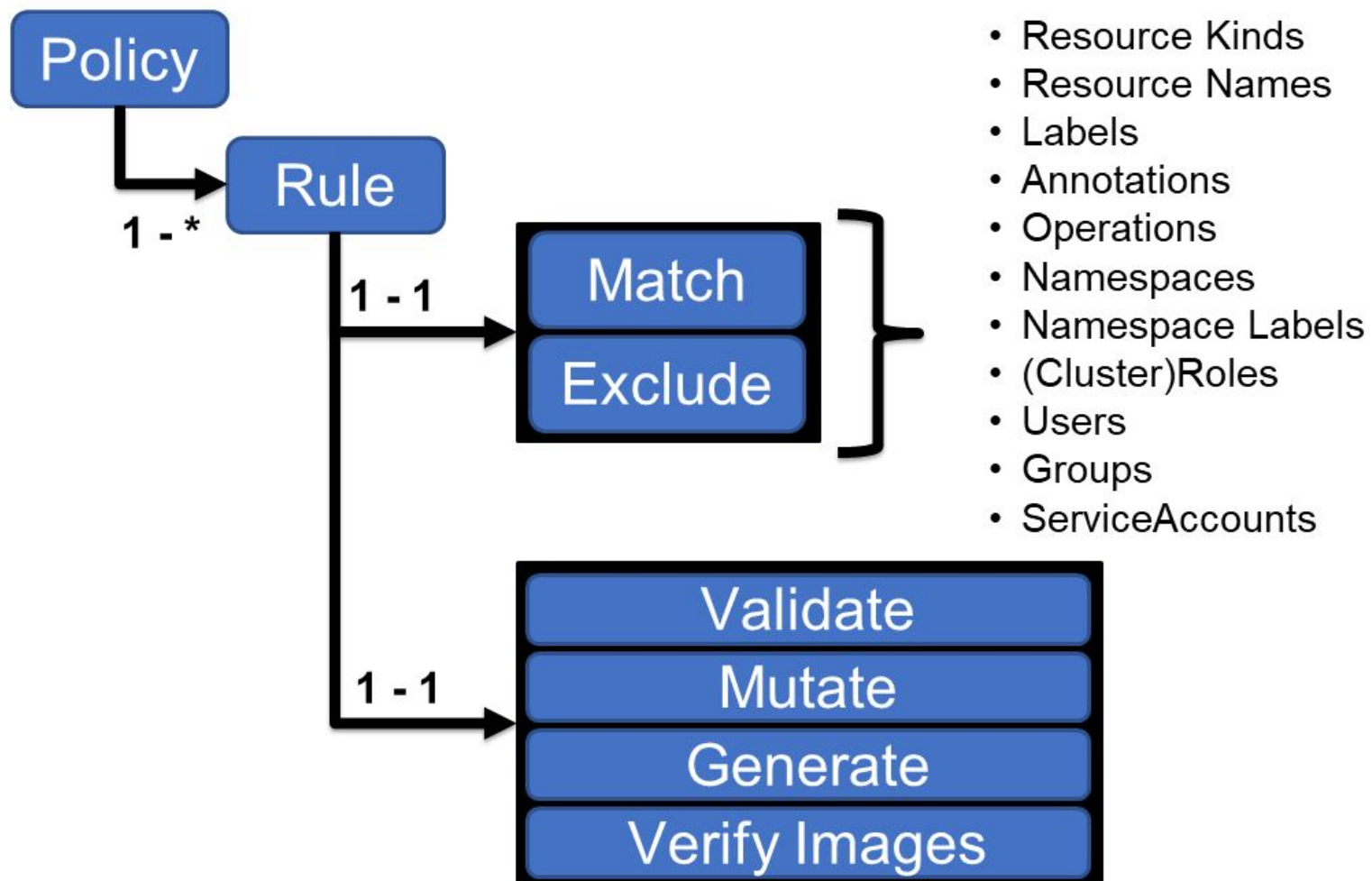
# Kyverno architecture



- ✓ Admission Controller
- ✓ Background Scanner
- ✓ CLI for static analysis



# A Kyverno policy




# A VerifyImages policy

```
apiVersion: kyverno.io/v2beta1
kind: ClusterPolicy
metadata:
  name: check-image-signature
spec:
  validationFailureAction: Enforce
  webhookTimeoutSeconds: 30
  failurePolicy: Fail
  rules:
    - name: verify-image-signature
      match:
        any:
          - resources:
              kinds:
                - Pod
      verifyImages:
        - type: Notary
          imageReferences:
            - "ghcr.io/kyverno/test-verify-image*"
          attestors:
            - count: 1
              entries:
                - certificates: |-
                    -----BEGIN PUBLIC KEY-----
                    MFkwEwYHKOZIzj0CAQYIKoZIzj0DAQcDQgAE8nXRh950IZbRj8Ra/N9sbq0PZrfM
                    5/KAQN0/KjHcorm/J5yctVd7iEcnessRQjU917hmK06JWVGHPDguIyakZA==
                    -----END PUBLIC KEY-----
```

```
apiVersion: kyverno.io/v2beta1
kind: ClusterPolicy
metadata:
  name: check-image-signature
```

# A VerifyImages policy

```
apiVersion: kyverno.io/v2beta1
kind: ClusterPolicy
metadata:
  name: check-image-signature
spec:
  validationFailureAction: Enforce
  webhookTimeoutSeconds: 30
  failurePolicy: Fail
  rules:
    - name: verify-image-signature
      match:
        any:
          - resources:
              kinds:
                - Pod
      verifyImages:
        - type: Notary
          imageReferences:
            - "ghcr.io/kyverno/test-verify-image*"
          attestors:
            - count: 1
              entries:
                - certificates: |-
                    -----BEGIN PUBLIC KEY-----
                    MFkwEwYHKOZIzj0CAQYIKoZIzj0DAQcDQgAE8nXRh950IZbRj8Ra/N9sbq0PZrfM
                    5/KAQN0/KjHcorm/J5yctVd7iEcnessRQjU917hmK06JWVGHPDguIyakZA==
                    -----END PUBLIC KEY-----
```



```
spec:
  validationFailureAction: Enforce
  webhookTimeoutSeconds: 30
  failurePolicy: Fail
```



# A VerifyImages policy

```
apiVersion: kyverno.io/v2beta1
kind: ClusterPolicy
metadata:
  name: check-image-signature
spec:
  validationFailureAction: Enforce
  webhookTimeoutSeconds: 30
  failurePolicy: Fail
  rules:
    - name: verify-image-signature
      match:
        any:
          - resources:
              kinds:
                - Pod
      verifyImages:
        - type: Notary
          imageReferences:
            - "ghcr.io/kyverno/test-verify-image*"
          attestors:
            - count: 1
              entries:
                - certificates: |-
                    -----BEGIN PUBLIC KEY-----
                    MFkwEwYHKOZIZj0CAQYIKoZIZj0DAQcDQgAE8nXRh950IZbRj8Ra/N9sbq0PZrfM
                    5/KAQN0/KjHcorm/J5yctVd7iEcnessRQjU917hmK06JWVGHPDguIyakZA==
                    -----END PUBLIC KEY-----
```

```
rules:
  - name: verify-image-signature
    match:
      any:
        - resources:
            kinds:
              - Pod
```

# A VerifyImages policy

```
apiVersion: kyverno.io/v2beta1
kind: ClusterPolicy
metadata:
  name: check-image-signature
spec:
  validationFailureAction: Enforce
  webhookTimeoutSeconds: 30
  failurePolicy: Fail
  rules:
```

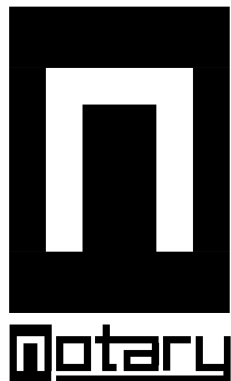
- name: verify-image-signature
 match:
 any:
 - resources:
 kinds:
 - Pod

```
  verifyImages:
    - type: Notary
      imageReferences:
        - "ghcr.io/kyverno/test-verify-image*"
      attestors:
        - count: 1
          entries:
            - certificates: |-
                -----BEGIN PUBLIC KEY-----
                MFkwEwYHKOZIzj0CAQYIKoZIzj0DAQcDQgAE8nXRh950IZbRj8Ra/N9sbq0PZrfM
                5/KAQN0/KjHcorm/J5yctVd7iEcnessRQjU917hmK06JWVGHPDguIyakZA==
                -----END PUBLIC KEY-----
```

```
  verifyImages:
    - type: Notary
      imageReferences:
        - "ghcr.io/kyverno/test-verify-image*"
      attestors:
        - count: 1
          entries:
            - certificates: |-
```

# What is Notary Project/Notation

## Ensure software authenticity and integrity



- ❑ Sign software artifacts
- ❑ Verify artifact with fine-grained trust policy
- ❑ Provides CLI, library, standard-based spec
- ❑ Support multiple plugins (Azure, AWS, Vault, Venafi)
- ❑ Integration with CI/CD (GitHub Actions, Azure DevOps)

## Adopted and contributed by



Notation CLI Command Sets	
notation certificate:	Manage certificates in trust store
notation key:	Manage keys used for signing
notation list:	List signatures of the signed artifact
notation login:	Log in to the registry
notation logout:	Log out from the registry
notation plugin:	Manage plugins
notation sign:	Sign artifacts
notation verify:	Verify OCI artifacts
notation version:	Show the notation version information



KubeCon



CloudNativeCon

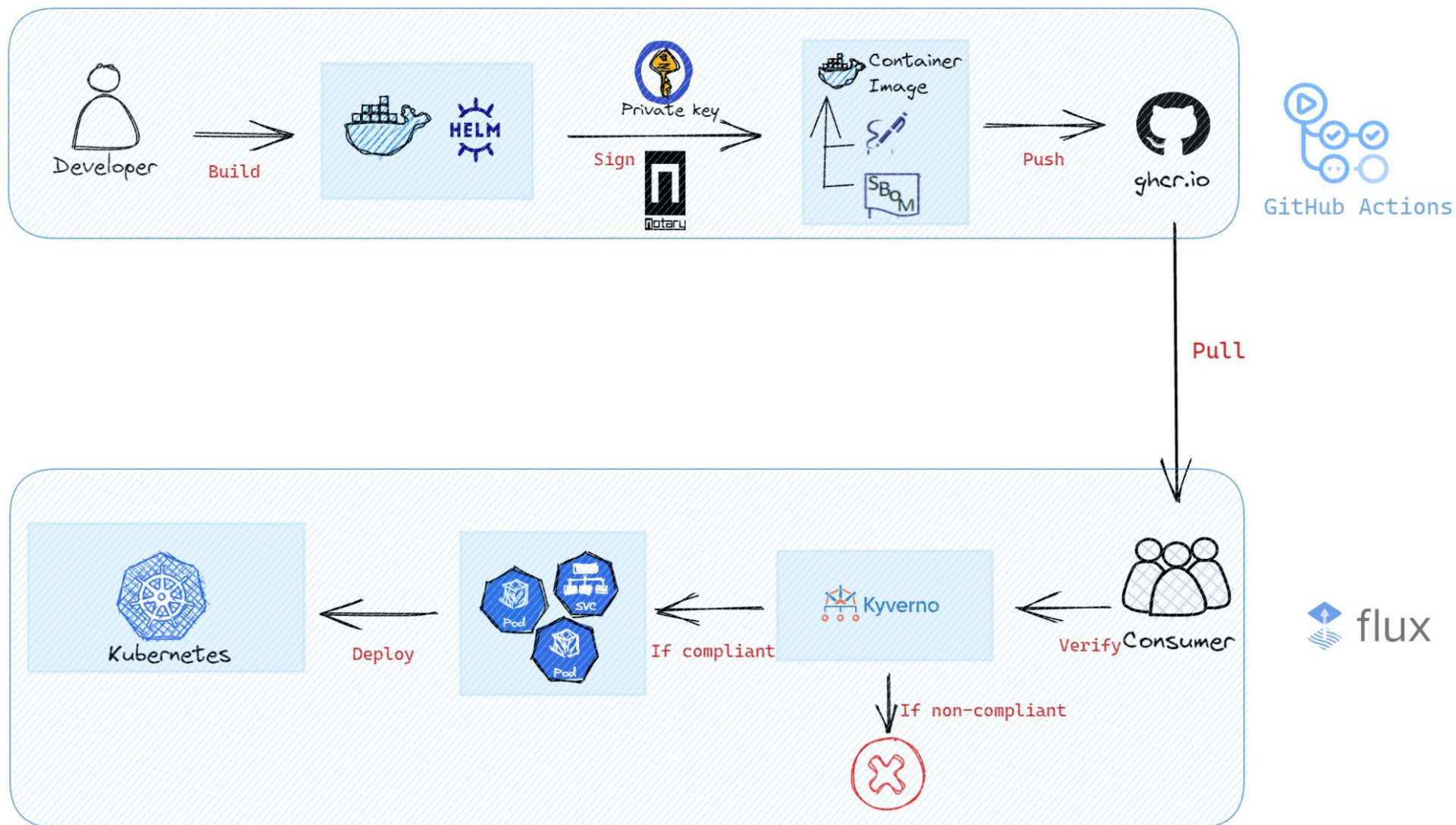


OPEN SOURCE SUMMIT

China 2023

# End-to-end demo: sign and verify images on Kubernetes with Notation and Kyverno in GitOps





# Join our communities



KubeCon



CloudNativeCon



OPEN SOURCE SUMMIT

China 2023

- Kyverno: <https://kyverno.io>
- Notation: <https://notaryproject.dev>
- ORAS: <https://oras.land>



KubeCon



CloudNativeCon



OPEN SOURCE SUMMIT

China 2023

# Q & A