KubeCon | CloudNativeCon

China 2025

KubeCon | CloudNativeCon

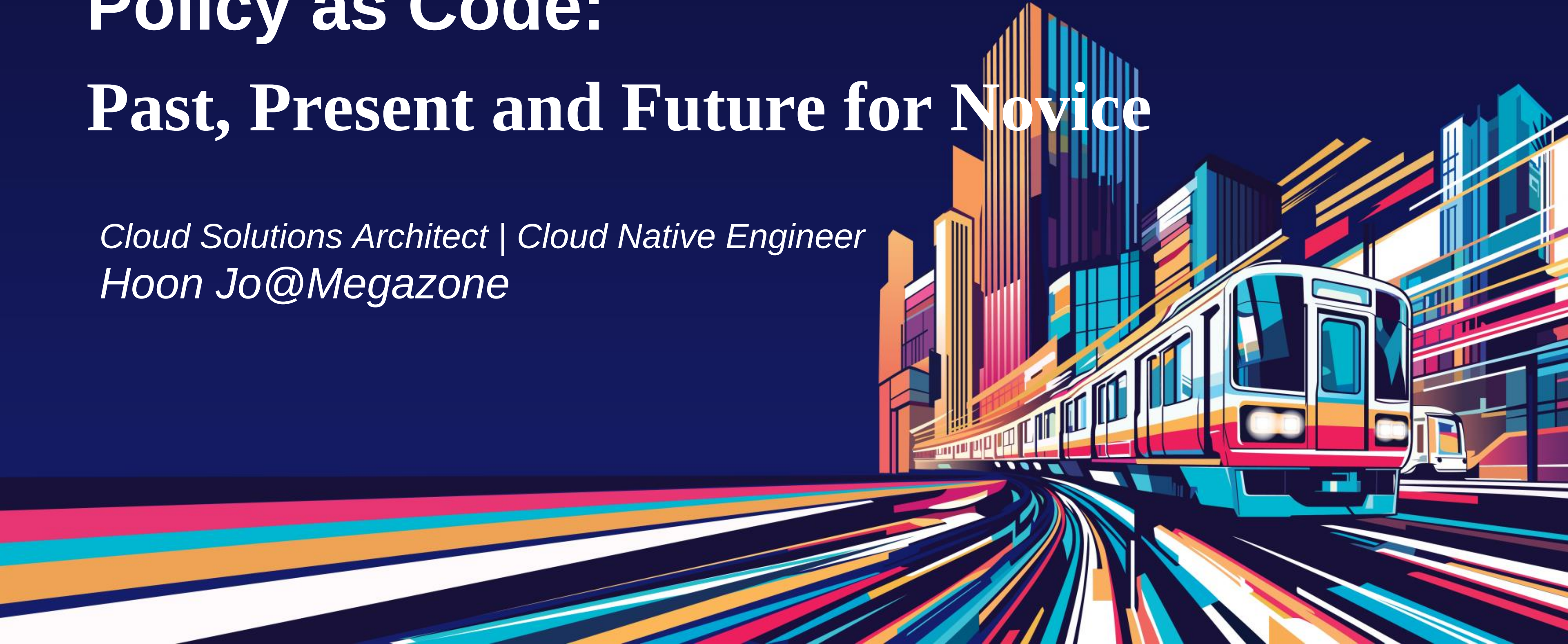
China 2025

Policy as Code:

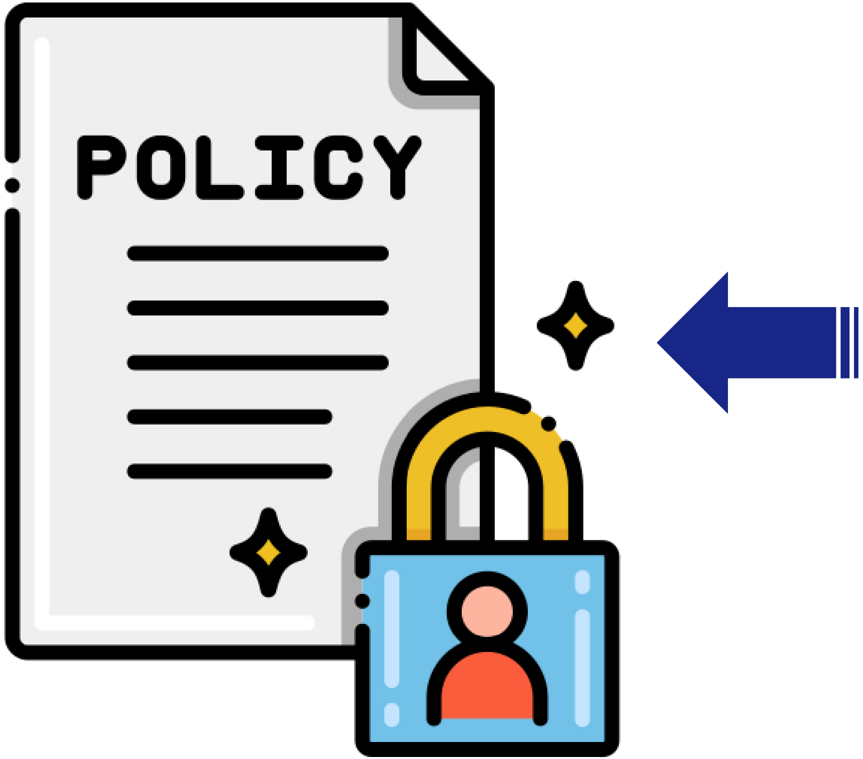
Past, Present and Future for Novice

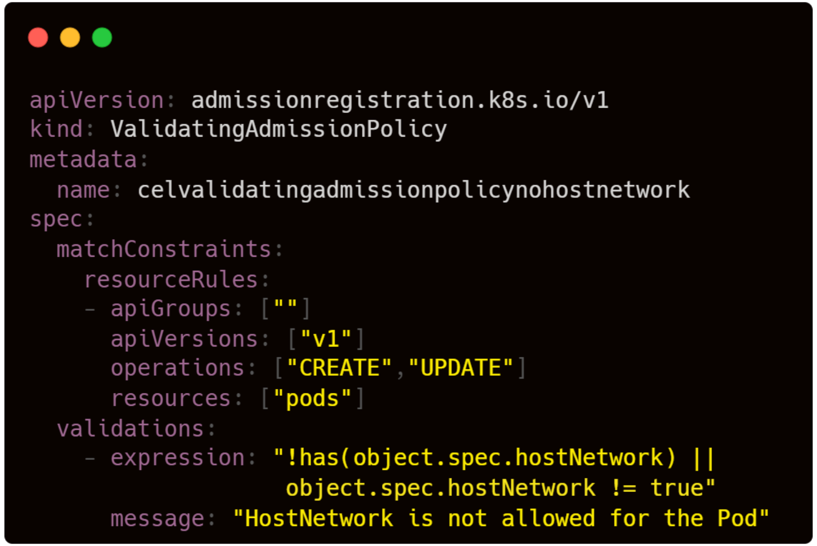
Cloud Solutions Architect | Cloud Native Engineer

Hoon Jo@Megazone



Policy as Code (PaC)





```yaml
apiVersion: admissionregistration.k8s.io/v1
kind: ValidatingAdmissionPolicy
metadata:
  name: celvalidatingadmissionpolicynohostnetwork
spec:
  matchConstraints:
    resourceRules:
    - apiGroups: [""]
      apiVersions: ["v1"]
      operations: ["CREATE","UPDATE"]
      resources: ["pods"]
  validations:
    - expression: "!has(object.spec.hostNetwork) ||
                   object.spec.hostNetwork != true"
      message: "HostNetwork is not allowed for the Pod"
```

AMBASSADOR

CLOUD NATIVE COMPUTING FOUNDATION

TAG ENVIRONMENTAL SUSTAINABILITY
MEETUP ORGANIZER
2023
KubeCon CloudNativeCon North America 2023
PROGRAM COMMITTEE MEMBER
2023
KubeCon CloudNativeCon OPEN SOURCE SUMMIT AI_dev China 2024
PROGRAM COMMITTEE
2024
KubeCon CloudNativeCon India 2024
PROGRAM COMMITTEE
2024
KubeCon CloudNativeCon Europe 2025
PROGRAM COMMITTEE MEMBER
2025
KubeCon CloudNativeCon China 2025
PROGRAM COMMITTEE MEMBER
2025
KubeCon CloudNativeCon India 2025
PROGRAM COMMITTEE MEMBER
2025
KUBERNETES COMMUNITY DAYS
KCD Korea
CONTRIBUTOR
(SPEAKER | COMMITTEE)
2023
Kubernetes Community Days Taiwan 2023
CLOUD NATIVE TAIWAN USER GROUP
KCD Contributor
TAG ENVIRONMENTAL SUSTAINABILITY
SPEAKER
2023
KubeCon CloudNativeCon North America 2023
SPEAKER
2023
KubeCon CloudNativeCon OPEN SOURCE SUMMIT AI_dev China 2024
SPEAKER
2024
KubeCon CloudNativeCon India 2024
SPEAKER
2024
KubeCon CloudNativeCon Europe 2025
SPEAKER
2025

Who am I ?

kubestronaut

https://github.com/SysNet4Admin

https://www.linkedin.com/in/hoonjo/

Intro

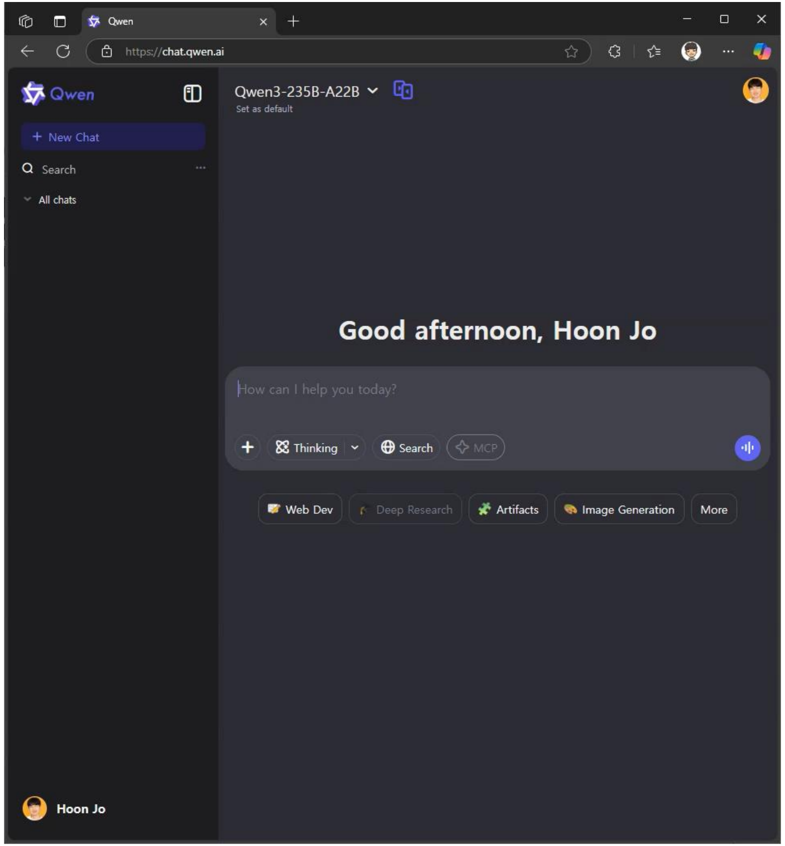
Why? As Code?

Benefits of Policy as Code

Benefit Category	Key Advantages	Impact
Consistency & Standardization	• Eliminates human inconsistency • Standardized enforcement • Reduces interpretation errors • Uniform validation	Uniform policy application across all environments regardless of operator
Automation & Efficiency	• Automated enforcement • Rapid feedback loops • Shift-left security • Reduced manual reviews	Faster development cycles with fewer security bottlenecks
Version Control & Governance	• Change tracking • Pull request reviews • Complete audit trail • Rollback capability	Transparent history of policy changes with accountability
Testing & Validation	• Testable policies • Simulation mode • Pre-deployment validation • Automated regression testing	Confidence in policy effectiveness before implementation
Integration DevOps	• CI/CD integration • IaC compatibility • Developer-friendly feedback • API-driven	Seamless incorporation into existing development workflows
Scalability & Complexity	• Scales with infrastructure • Centralized management • Handles sophisticated rules • Policy reuse	Maintains effectiveness as environments grow more complex
Compliance & Governance	• Demonstrable compliance • Regulatory adaptability • Continuous verification • Living documentation	Simplified audits and faster response to regulatory changes
Organization Improvement	• Knowledge transfer • Clearer communication • Organizational learning • Cross-team collaboration	Better alignment between security, development, and operations
Risk Reduction	• Preventative controls • Reduced manual errors • Consistent security posture • Configuration drift prevention	Lower likelihood of security incidents and compliance violations

Everything as Code (EaC) well-fitted w/ AI

Policy as Code	**(PaC)**
Configuration as Code	(CaC)
Security as Code	(SaC)
Compliance as Code	(CaC)
Network as Code	(NaC)
Database as Code	(DaC)
Monitoring as Code	(MaC)
Pipeline as Code	(PaC)
Documentation as Code	(DaC)
Disaster Recovery as Code	(DRaC)



Good afternoon, Hoon Jo

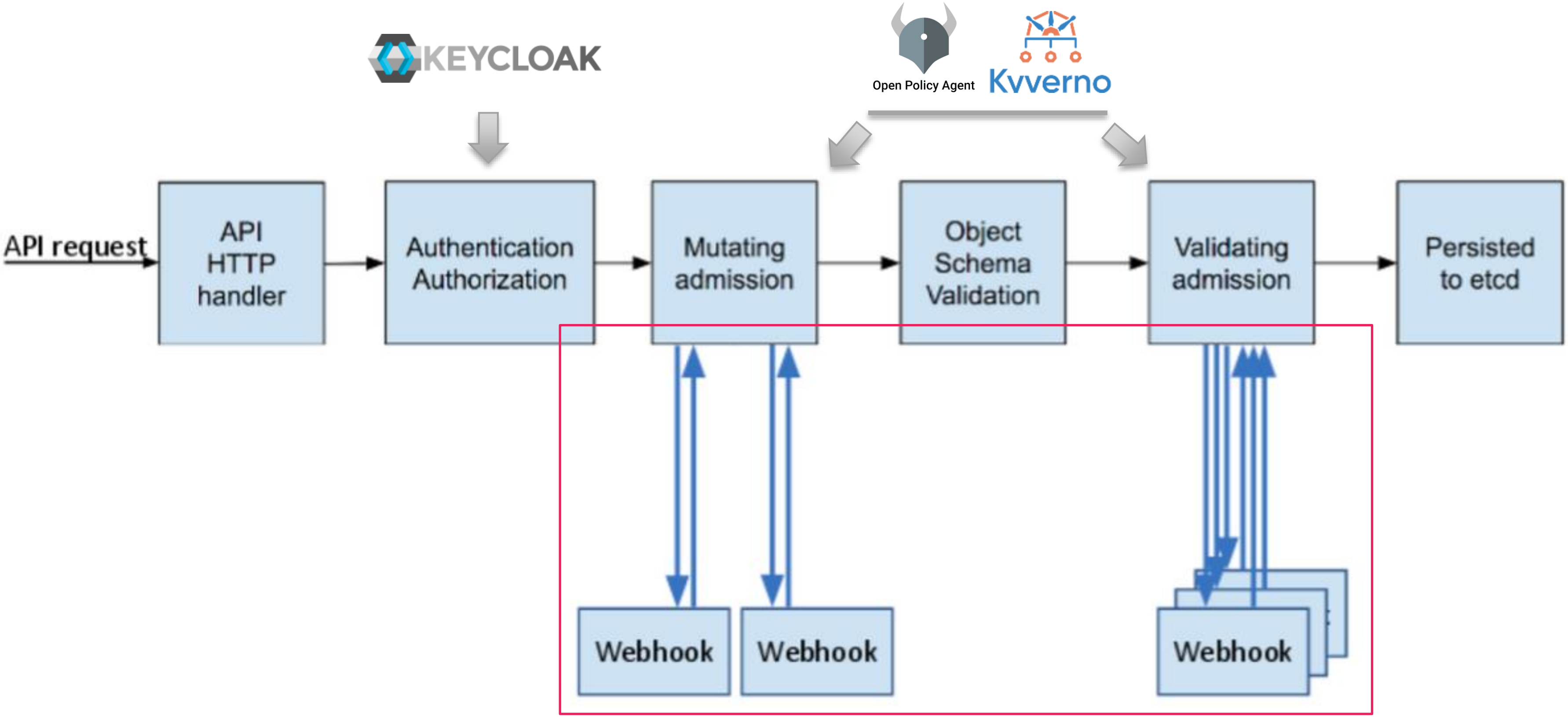
How can I help you today?

But… AI generates Code and then?

PART I

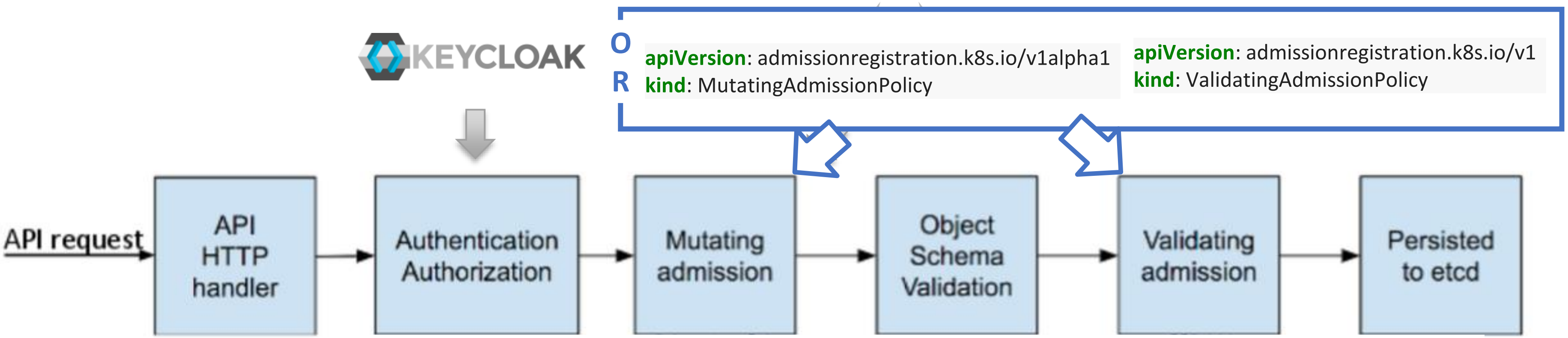
PaC: Past

Admission-Controllers by Policy as Code



https://kubernetes.io/blog/2019/03/21/a-guide-to-kubernetes-admission-controllers/

Chg: Admission-Controllers by PaC w/o Webhook

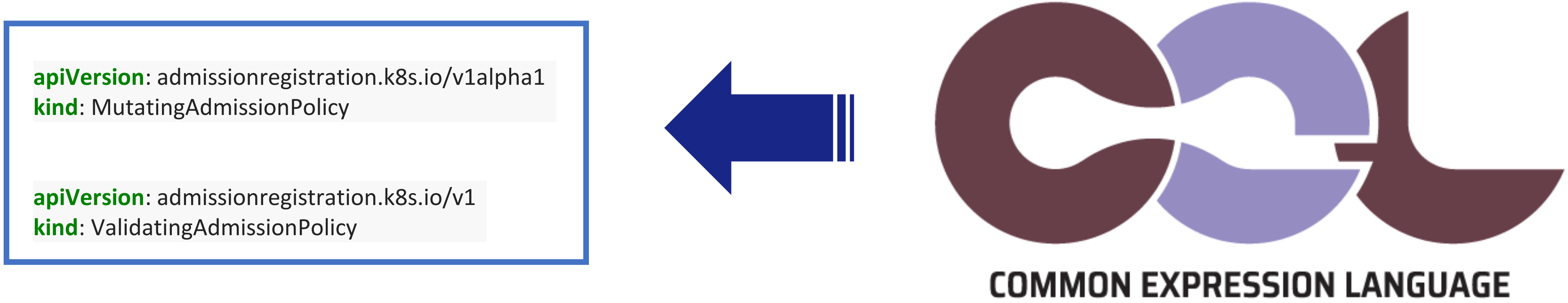


```
apiVersion: admissionregistration.k8s.io/v1alpha1
kind: MutatingAdmissionPolicy
```

```
apiVersion: admissionregistration.k8s.io/v1
kind: ValidatingAdmissionPolicy
```

https://kubernetes.io/blog/2019/03/21/a-guide-to-kubernetes-admission-controllers/

By CEL(Common Expression Language)

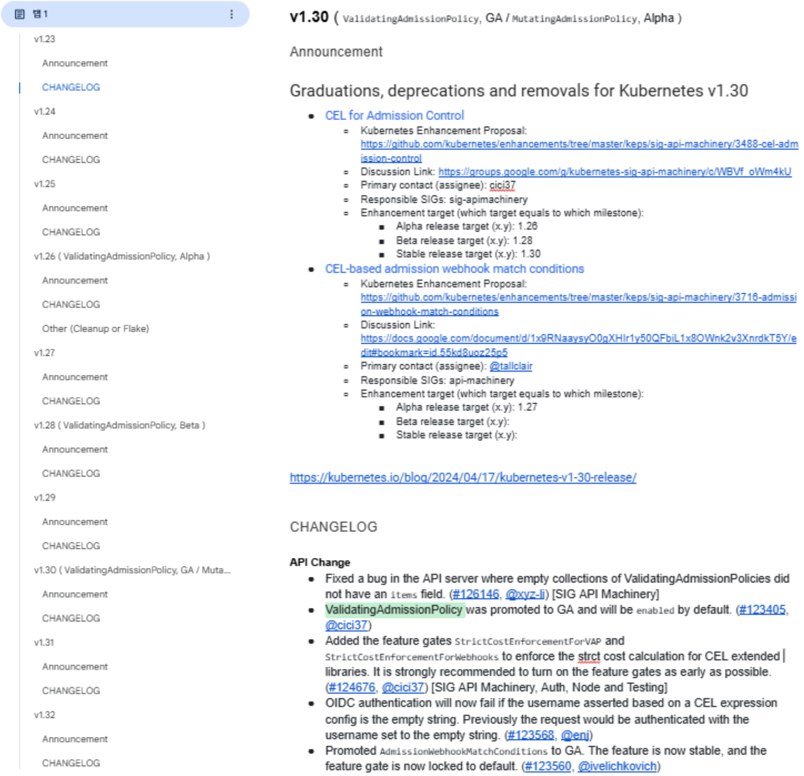


```
apiVersion: admissionregistration.k8s.io/v1alpha1
kind: MutatingAdmissionPolicy
```

```
apiVersion: admissionregistration.k8s.io/v1
kind: ValidatingAdmissionPolicy
```

The history of CEL into the Kubernetes

cel-spec Public



탭 1

- v1.23
  - Announcement
  - CHANGELOG
- v1.24
  - Announcement
  - CHANGELOG
- v1.25
  - Announcement
  - CHANGELOG
- v1.26 (ValidatingAdmissionPolicy, Alpha)
  - Announcement
  - CHANGELOG
  - Other (Cleanup or Flake)
- v1.27
  - Announcement
  - CHANGELOG
- v1.28 (ValidatingAdmissionPolicy, Beta)
  - Announcement
  - CHANGELOG
- v1.29
  - Announcement
  - CHANGELOG
- v1.30 (ValidatingAdmissionPolicy, GA / Muta...
  - Announcement
  - CHANGELOG
- v1.31
  - Announcement
  - CHANGELOG
- v1.32
  - Announcement
  - CHANGELOG

v1.30 (`ValidatingAdmissionPolicy`, GA / `MutatingAdmissionPolicy`, Alpha)

Announcement

Graduations, deprecations and removals for Kubernetes v1.30

- CEL for Admission Control
  - Kubernetes Enhancement Proposal: https://github.com/kubernetes/enhancements/tree/master/keps/sig-api-machinery/3488-cel-admission-control
  - Discussion Link: https://groups.google.com/g/kubernetes-sig-api-machinery/c/WBVf_oWm4kU
  - Primary contact (assignee): cici37
  - Responsible SIGs: sig-apimachinery
  - Enhancement target (which target equals to which milestone):
    - Alpha release target (x.y): 1.26
    - Beta release target (x.y): 1.28
    - Stable release target (x.y): 1.30
- CEL-based admission webhook match conditions
  - Kubernetes Enhancement Proposal: https://github.com/kubernetes/enhancements/tree/master/keps/sig-api-machinery/3716-admission-webhook-match-conditions
  - Discussion Link: https://docs.google.com/document/d/1x9RNaaysyO0gXHIr1y50QFbiL1x8OWnk2v3XnrdkT5Y/edit#bookmark=id.55kd8uoz25p5
  - Primary contact (assignee): @tallclair
  - Responsible SIGs: api-machinery
  - Enhancement target (which target equals to which milestone):
    - Alpha release target (x.y): 1.27
    - Beta release target (x.y):
    - Stable release target (x.y):

https://kubernetes.io/blog/2024/04/17/kubernetes-v1-30-release/

CHANGELOG

API Change

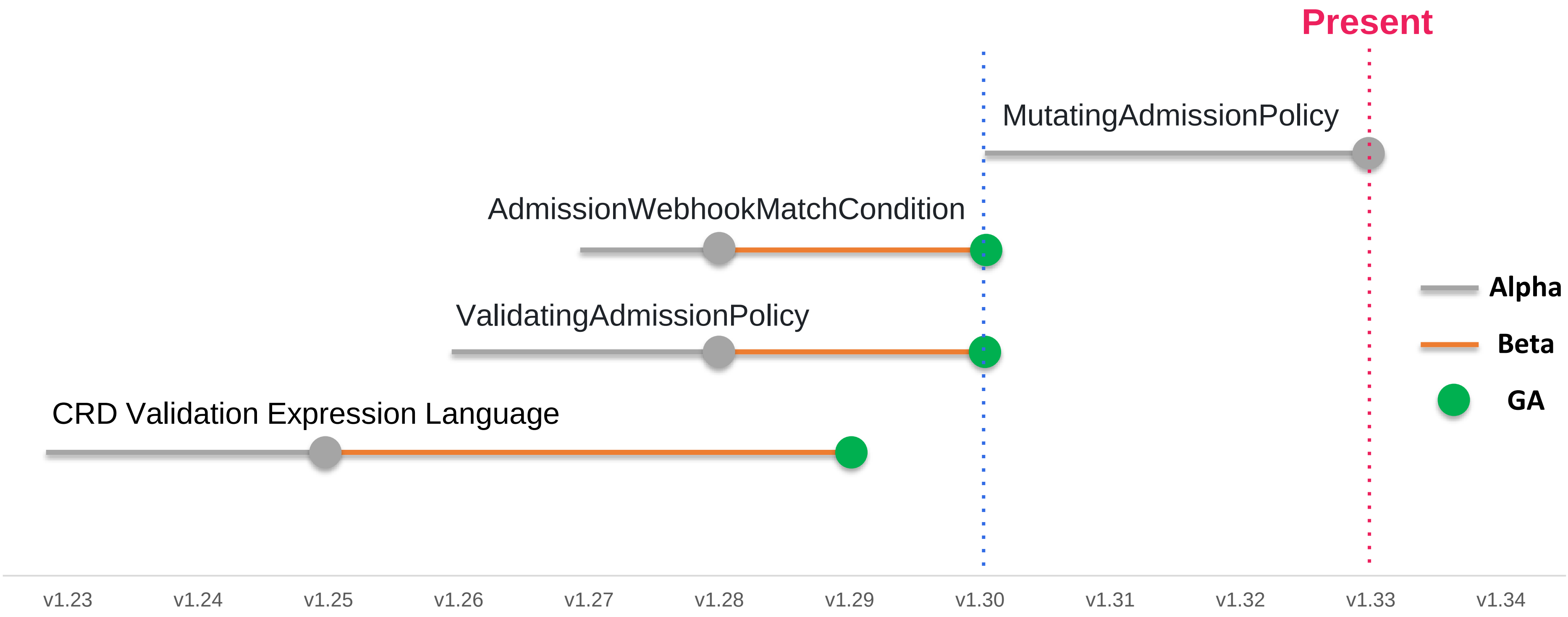
- Fixed a bug in the API server where empty collections of ValidatingAdmissionPolicies did not have an `items` field. (#126146, @xyz-li) [SIG API Machinery]
- ValidatingAdmissionPolicy was promoted to GA and will be `enabled` by default. (#123405, @cici37)
- Added the feature gates `StrictCostEnforcementForVAP` and `StrictCostEnforcementForWebhooks` to enforce the strct cost calculation for CEL extended libraries. It is strongly recommended to turn on the feature gates as early as possible. (#124676, @cici37) [SIG API Machinery, Auth, Node and Testing]
- OIDC authentication will now fail if the username asserted based on a CEL expression config is the empty string. Previously the request would be authenticated with the username set to the empty string. (#123568, @enj)
- Promoted `AdmissionWebhookMatchConditions` to GA. The feature is now stable, and the feature gate is now locked to default. (#123560, @ivelichkovich)

cel-go Public

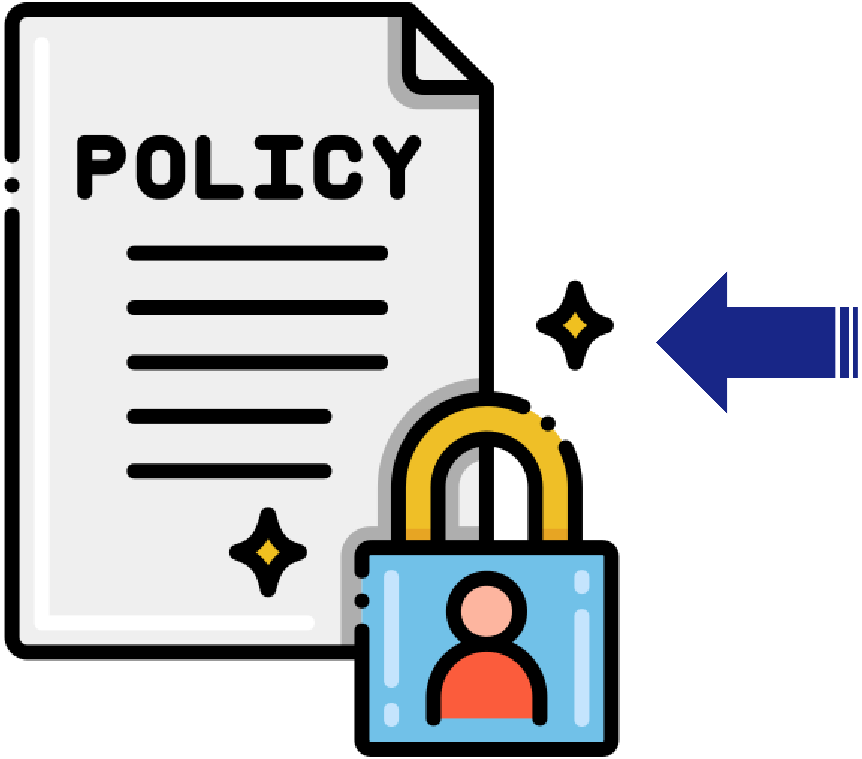
PART II

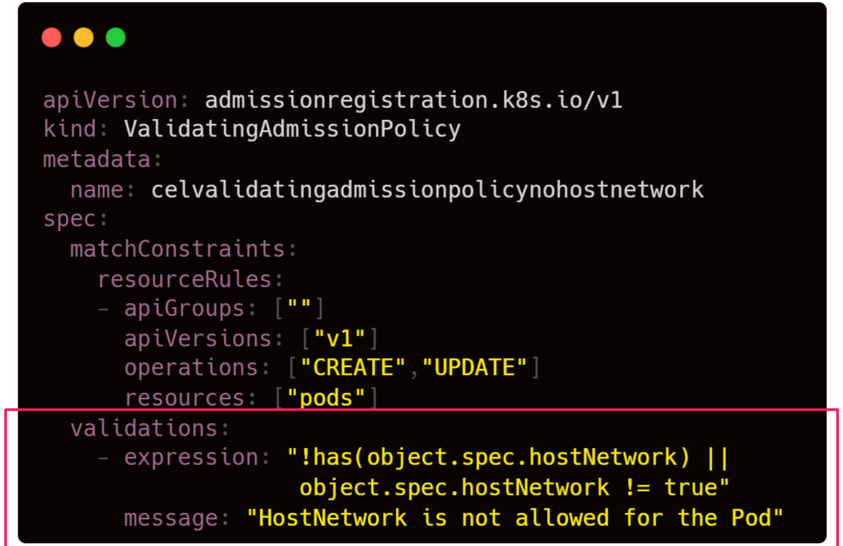
PaC: Present

Maturity: CEL & Admission



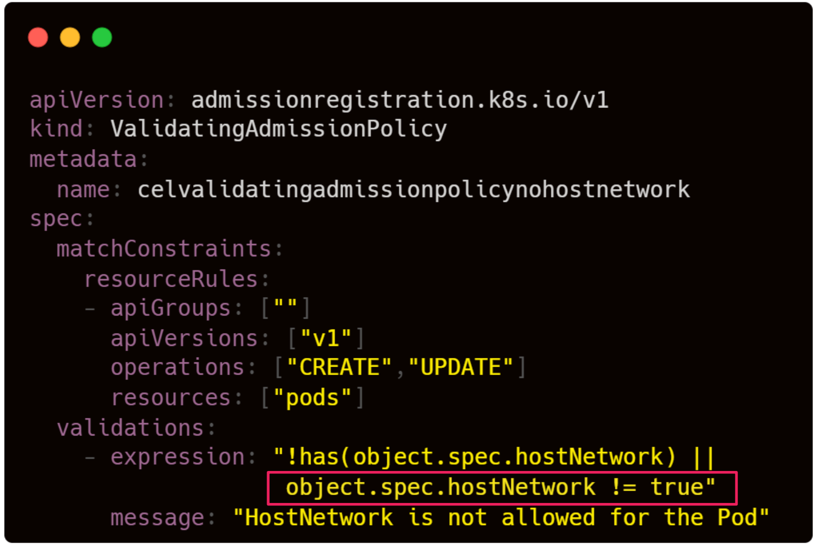
Policy as Code (PaC) by CEL in kubernetes





```yaml
apiVersion: admissionregistration.k8s.io/v1
kind: ValidatingAdmissionPolicy
metadata:
  name: celvalidatingadmissionpolicynohostnetwork
spec:
  matchConstraints:
    resourceRules:
    - apiGroups: [""]
      apiVersions: ["v1"]
      operations: ["CREATE","UPDATE"]
      resources: ["pods"]
  validations:
    - expression: "!has(object.spec.hostNetwork) ||
                   object.spec.hostNetwork != true"
      message: "HostNetwork is not allowed for the Pod"
```

ValidatingAdmissionPolicy’s expression



```yaml
apiVersion: admissionregistration.k8s.io/v1
kind: ValidatingAdmissionPolicy
metadata:
  name: celvalidatingadmissionpolicynohostnetwork
spec:
  matchConstraints:
    resourceRules:
    - apiGroups: [""]
      apiVersions: ["v1"]
      operations: ["CREATE","UPDATE"]
      resources: ["pods"]
  validations:
    - expression: "!has(object.spec.hostNetwork) ||
                   object.spec.hostNetwork != true"
      message: "HostNetwork is not allowed for the Pod"
```

```yaml
spec:
  containers:
  - image: quay.io/nginx/nginx-unprivileged
    imagePullPolicy: IfNotPresent
    name: nginx
    resources: {}
    terminationMessagePath: /dev/termination-log
    terminationMessagePolicy: File
    volumeMounts:
    - mountPath:
/var/run/secrets/kubernetes.io/serviceaccount
      name: kube-api-access-h7dj2
      readOnly: true
  dnsPolicy: ClusterFirst
  enableServiceLinks: true
  hostNetwork: true
  nodeName: w3-k8s
```

Sample: Policy as Code for others

Authentication

```
…
valid_token {
  tokens := split(input.headers["Authorization"][0], " ")
  …
  io.jwt.verify_hs256(token, "secret")
```

Authorization

```
…
rules:
- apiGroups: [""]
  resources: ["pods"]
  verbs: ["create", "get", "list"]
```

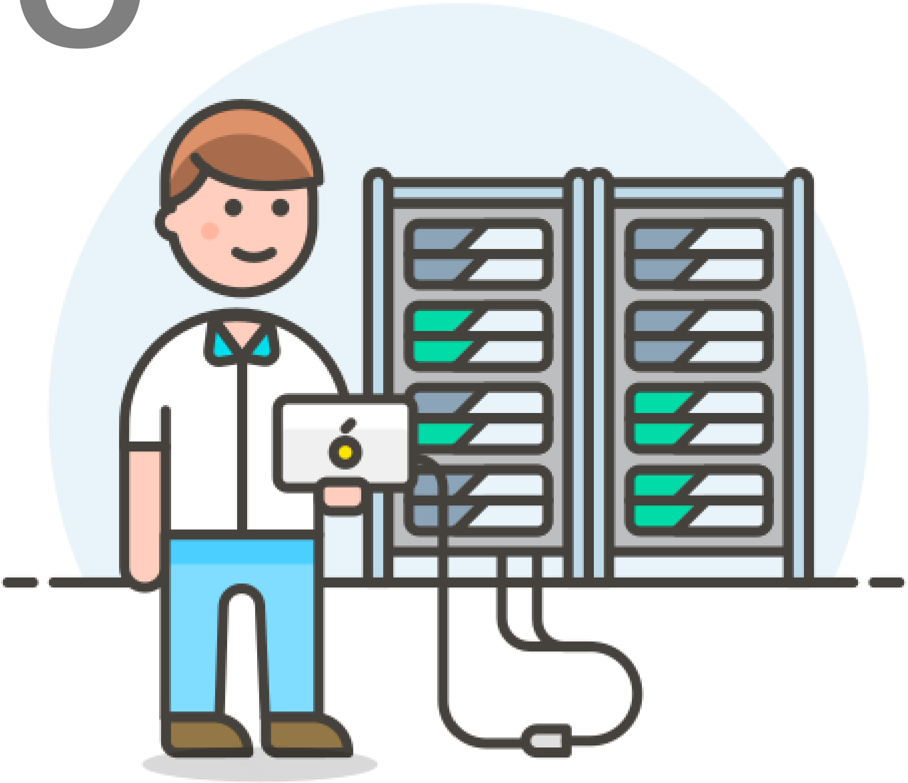
Mutation

```
…
matchConditions:
    - name: does-not-already-have-sidecar
      expression: "!object.spec.initContainers.exists(ic,
ic.name == \"mesh-proxy\")"
```

Validation

```
…
  validations:
    - expression: "!has(object.spec.hostNetwork) ||
                        object.spec.hostNetwork != true"
      message: "HostNetwork is not allowed for the Pod"
```

DEMO



COMMON EXPRESSION LANGUAGE

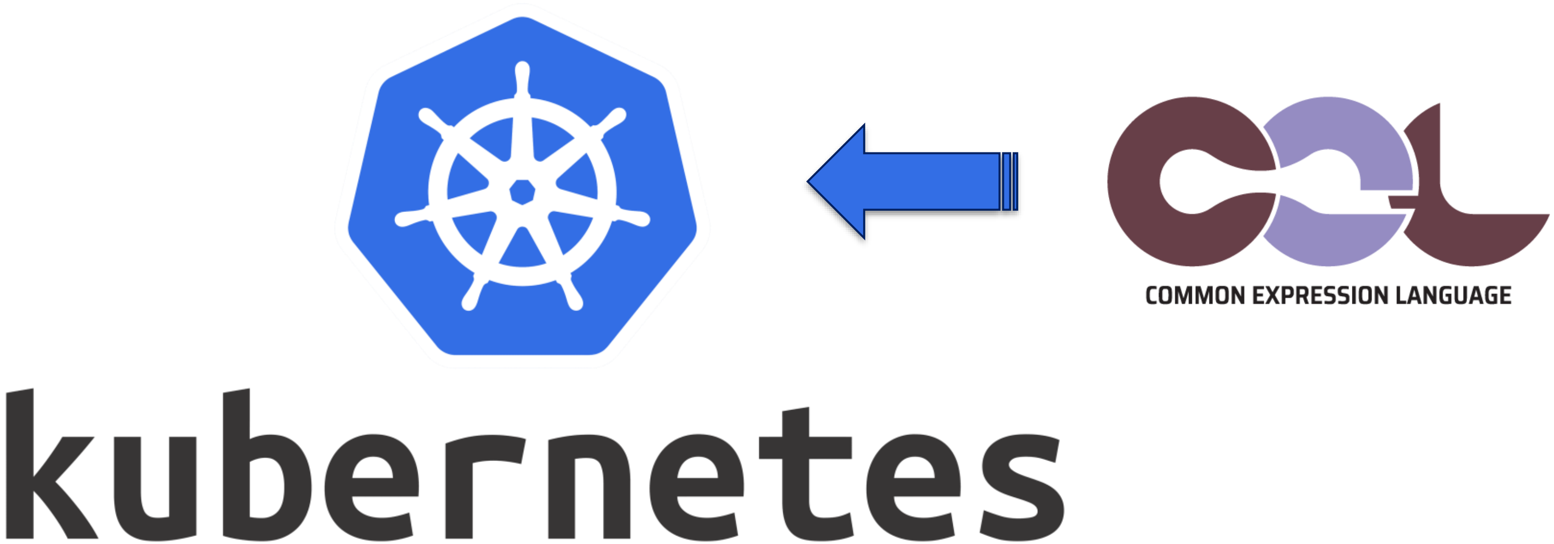
KubeCon | CloudNativeCon

China 2025

PART III

PaC: Future

CEL is already in k8s

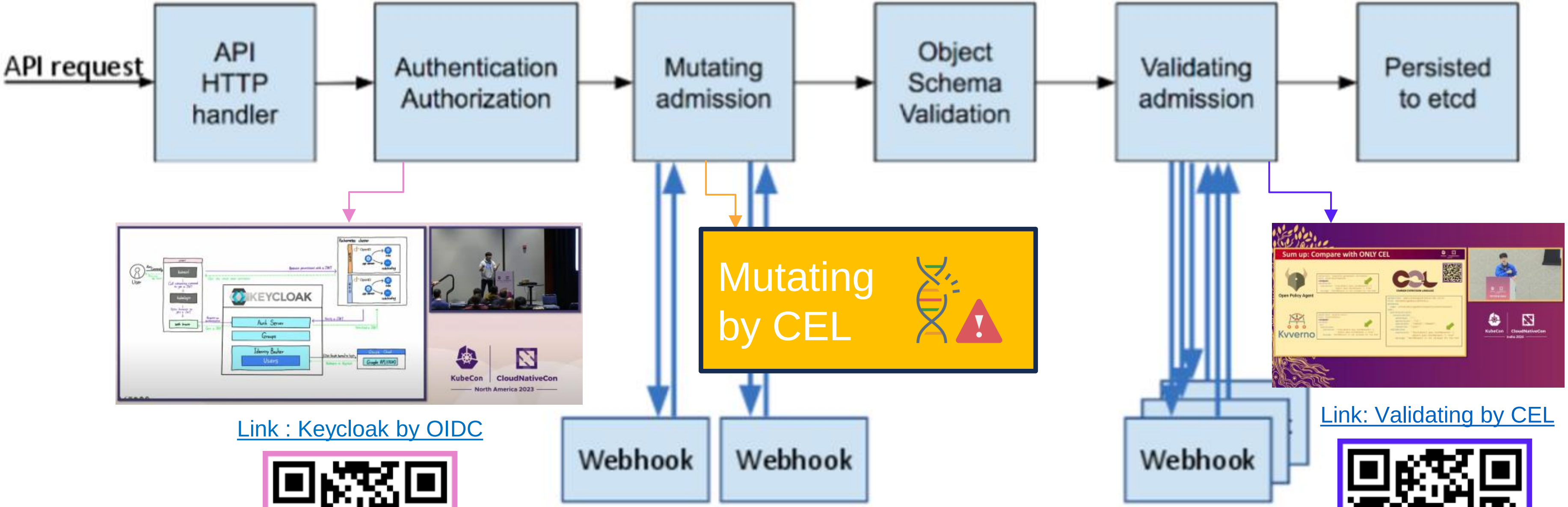


Something will implement by PaC (thru CEL)

OR

```
apiVersion: admissionregistration.k8s.io/v1alpha1
kind: MutatingAdmissionPolicy
```

```
apiVersion: admissionregistration.k8s.io/v1
kind: ValidatingAdmissionPolicy
```



Link : Keycloak by OIDC

Link: Validating by CEL

Any Questions?

KubeCon China 2025's docs

[KubeCon China 2025] #1 History of CEL into the Kubernetes

- ShortURL: https://m.site.naver.com/1HYFg

[KubeCon China 2025] #2 Validating admission by CEL

- ShortURL: https://m.site.naver.com/1HYRn

https://github.com/SysNet4Admin

https://www.linkedin.com/in/hoonjo/