OpenInfra DAYS KOREA

OpenInfra Days Korea 2025

Policy as Code의 과거 현재 그리고 미래

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

Who am I ?

kubestronaut

https://github.com/SysNet4Admin

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

OpenInfra DAYS KOREA

OpenInfra Days Korea 2025

Intro

왜? 코드로 할까요?

코드로 정책을 배포할 때 얻을 수 있는 이점들

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)는 AI 시대에 적합할까요?

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)

그런데 AI로 코드를 만들고 나면?

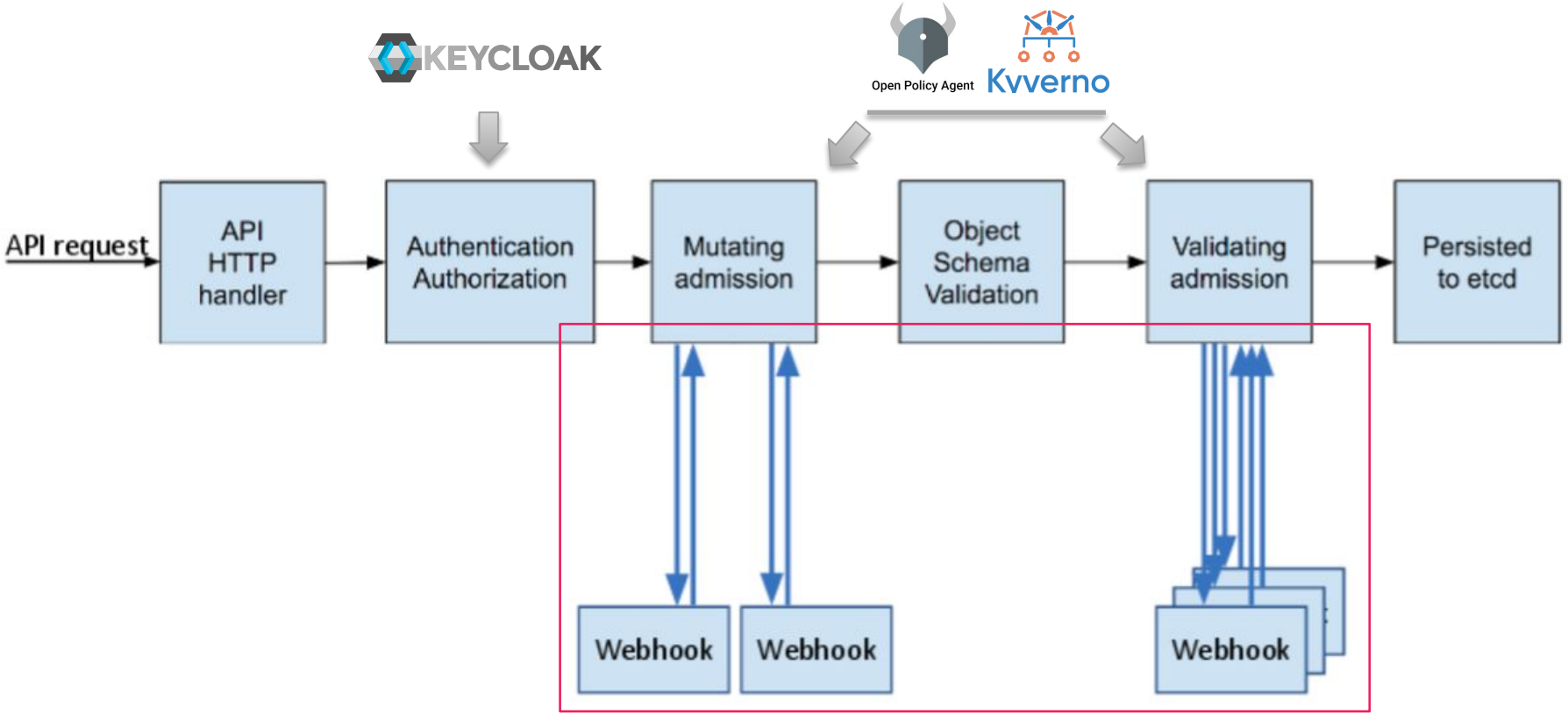
OpenInfra DAYS KOREA

OpenInfra Days Korea 2025

PART I

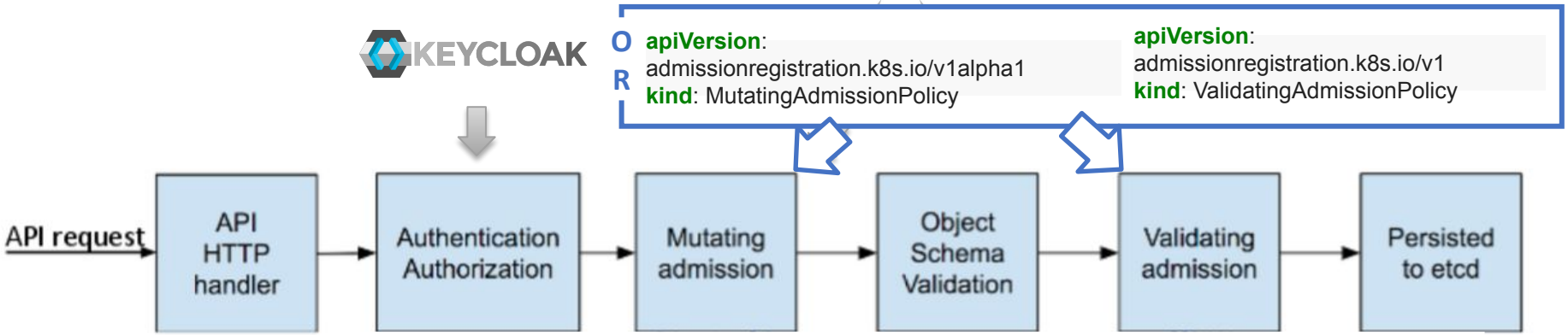
PaC: 과거

과거 : Admission-Controllers



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

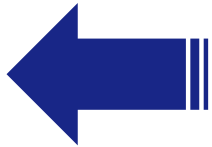
바뀜 : Admission-Controllers (웹훅이 없어도 동작 가능)

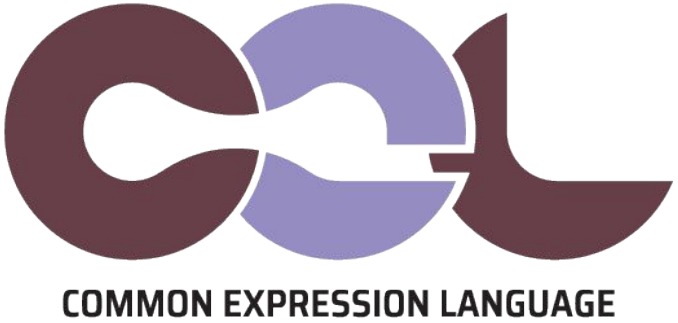


https://kubernetes.io/blog/2019/03/21/a-guide-to-kubernetes-admission-controllers/

언어는 CEL(Common Expression Language)

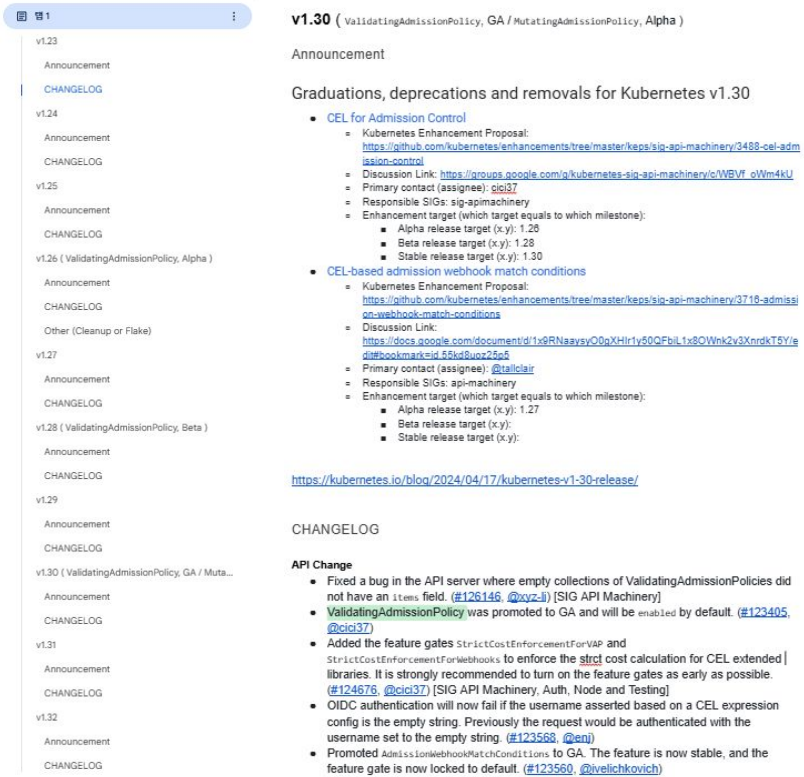
```
apiVersion:
admissionregistration.k8s.io/v1alpha1
kind: MutatingAdmissionPolicy

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





CEL이 쿠버네티스에 적용되기 까지 과정

cel-spec Public



cel-go Public

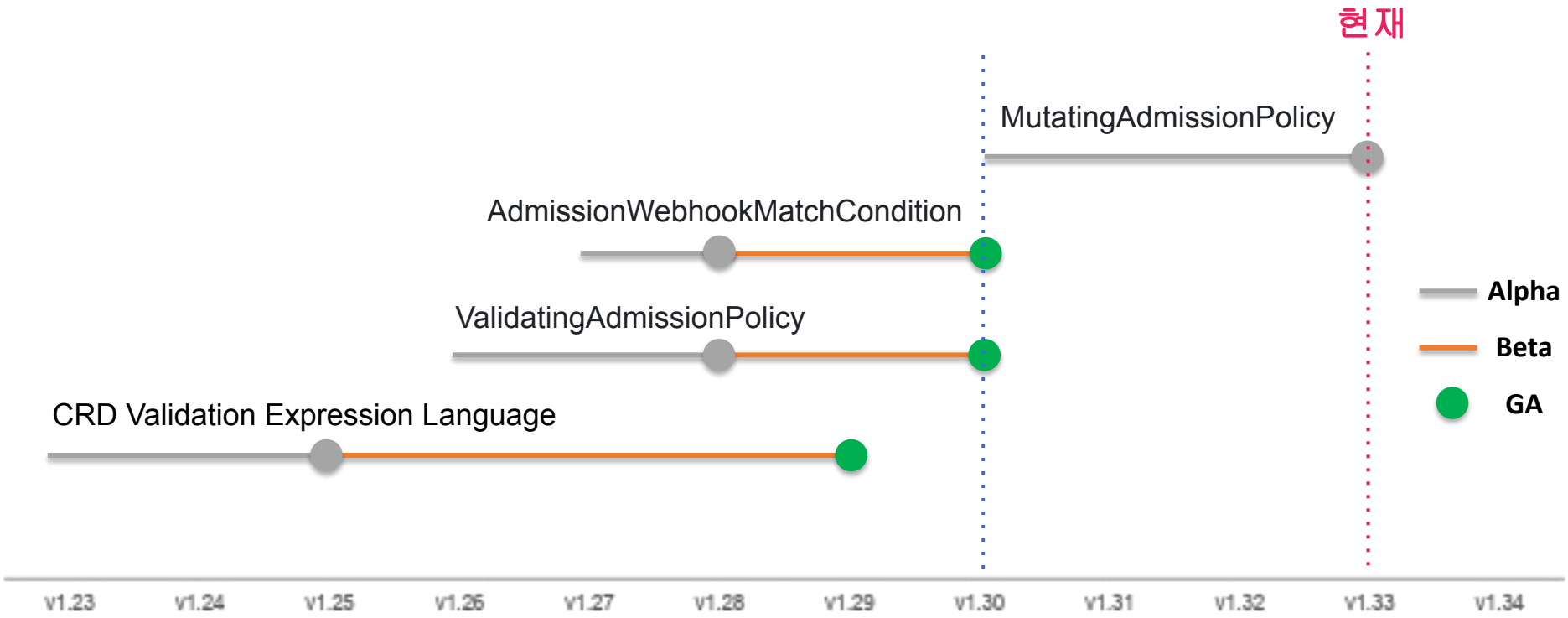
OpenInfra DAYS KOREA

OpenInfra Days Korea 2025

PART II

PaC: 현재

성숙도: CEL & Admission



Policy as Code (PaC) ← 쿠버네티스의 CEL


```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"
```

예제 : ValidatingAdmissionPolicy

```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
```

다른 예제: Policy as Code

Authentication

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

Authorization

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

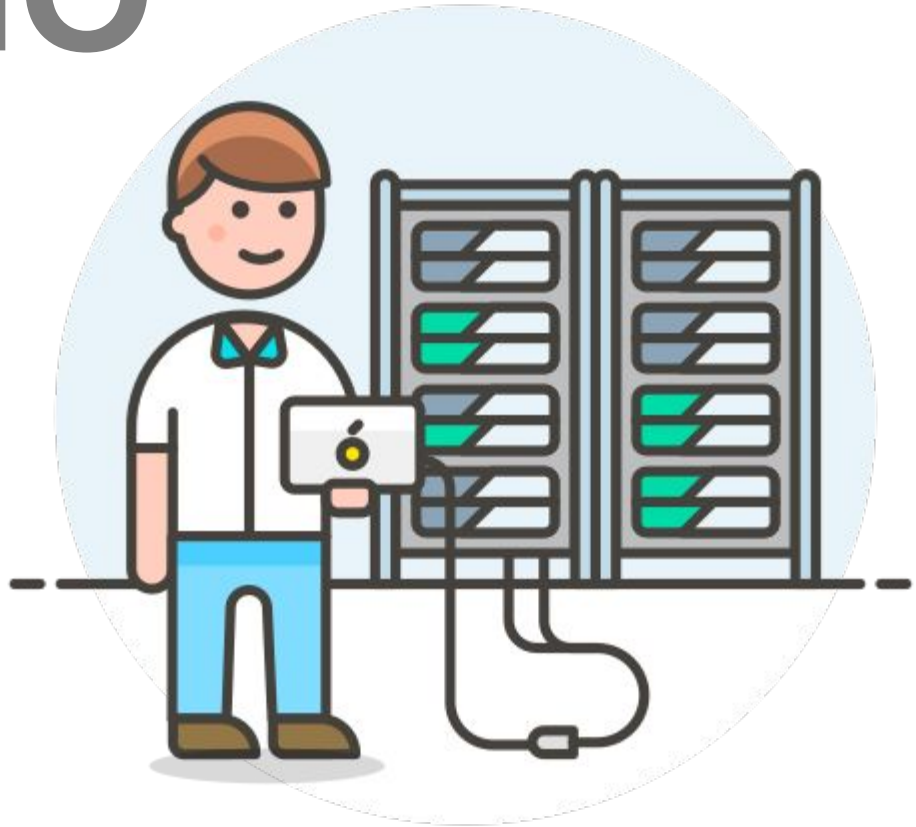
Mutation

```
...
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

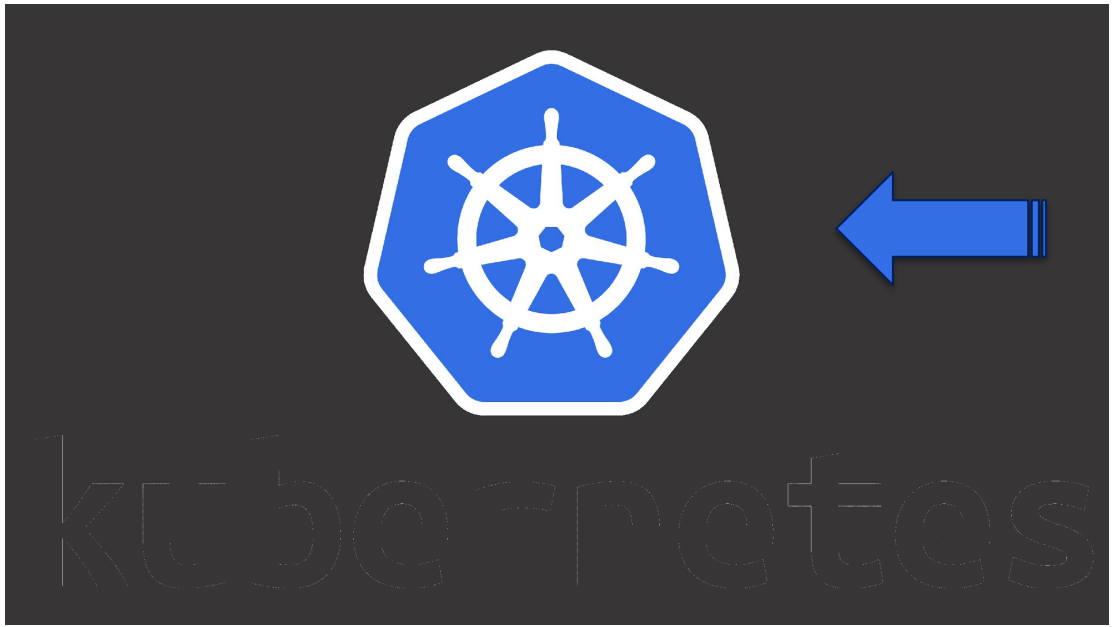
OpenInfra DAYS KOREA

OpenInfra Days Korea 2025

PART III

PaC: 미래

CEL은 이미 쿠버네티스에 적용됨



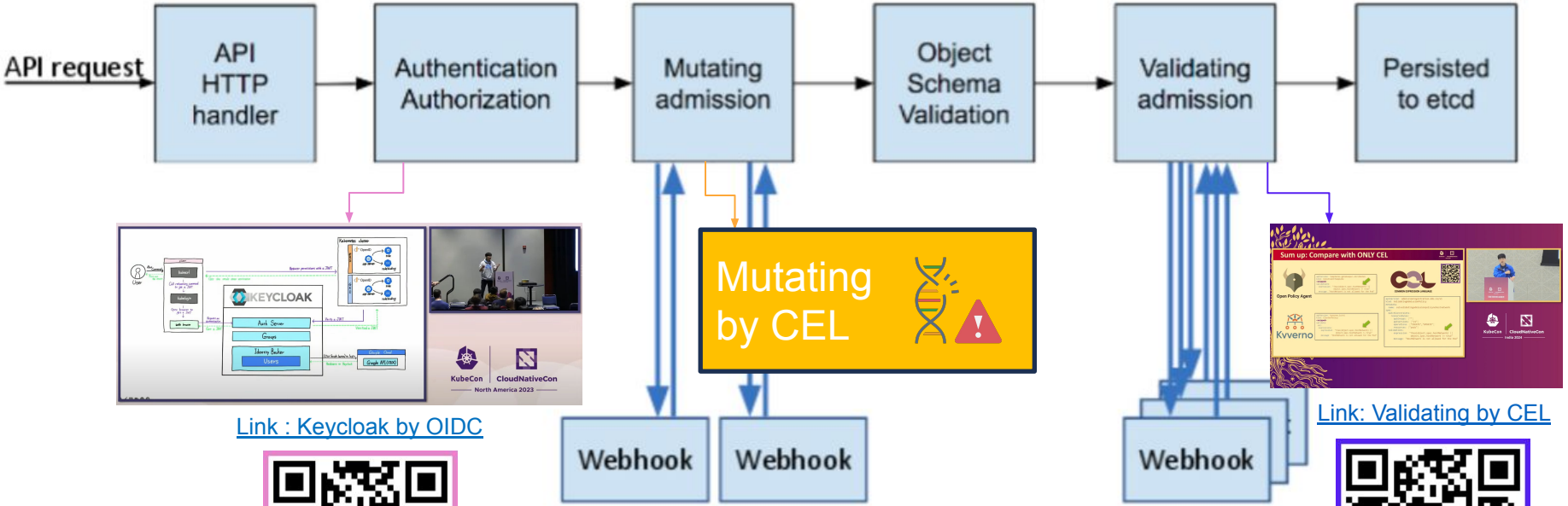
COMMON EXPRESSION LANGUAGE

이제 곧 무언가가 더 쿠버네티스로 들어옵니다!

O R

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

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



Link : Keycloak by OIDC

Link: Validating by CEL

질문을 원합니다! Plz

OpenInfra Days 2025's docs

#1 History of CEL into the Kubernetes

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

#2 Validating admission by CEL

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

https://github.com/SysNet4Admin

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