



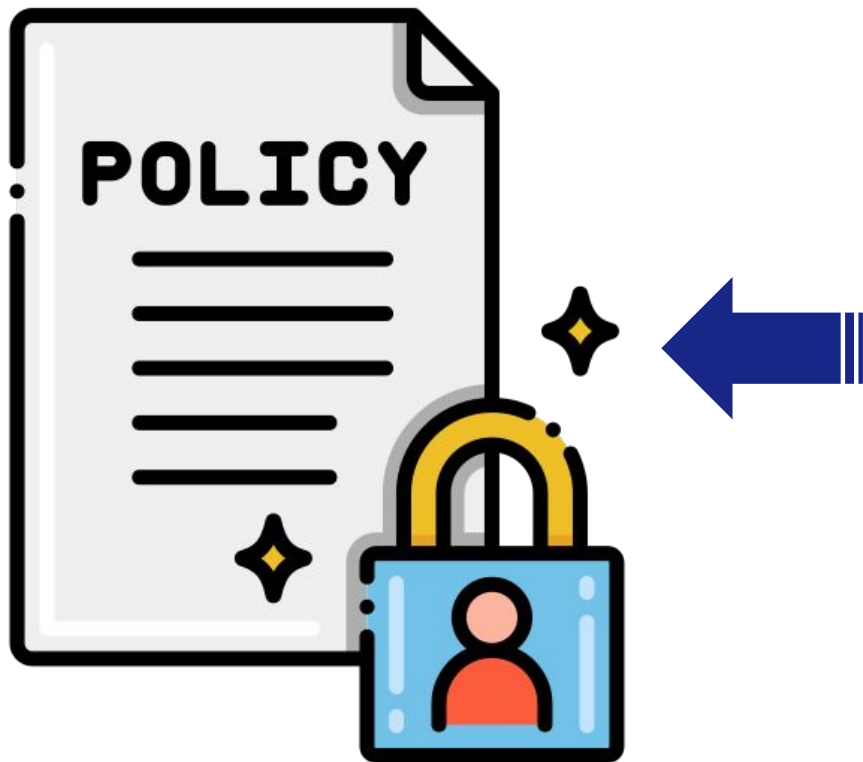
OpenInfra Days
Korea 2025

Policy as Code의 과거 현재 그리고 미래

Cloud Solutions Architect | Cloud Native Engineer
Hoon Jo@Megazone



Policy as Code (PaC)



```
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"
```



Who am I ?



<https://github.com/SysNet4Admin>



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

OpenInfra
DAYS



KOREA

OpenInfra Days
Korea 2025

Intro

왜? 코드로 할까요?

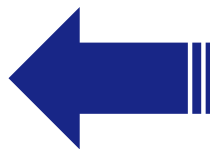


코드로 정책을 배포할 때 얻을 수 있는 이점들

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)



```
Gemini - mz01-hj
79% 13 GB 38 kB/s 5.1 kB/s

> GEMINI

Tips for getting started:
1. Ask questions, edit files, or run commands.
2. Be specific for the best results.
3. ./help for more information.

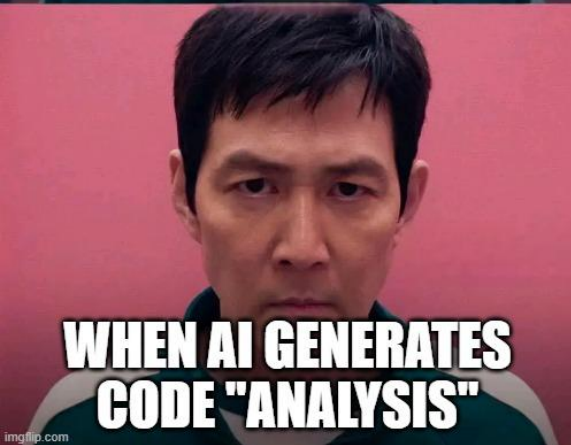
You are running Gemini CLI in your home directory. It is recommended to run in a
project-specific directory.

Using 1 GEMINI.md file
> | Type your message or @path/to/file

~ no sandbox (see /docs) gemini-2.5-flash (99% context left)
```

그런데 AI로 코드를 만들고 나면?

WHEN AI GENERATES CODE



I DON'T KNOW WHAT TO DO



BUT I DON'T KNOW WHAT TO DO



OpenInfra
DAYS



KOREA

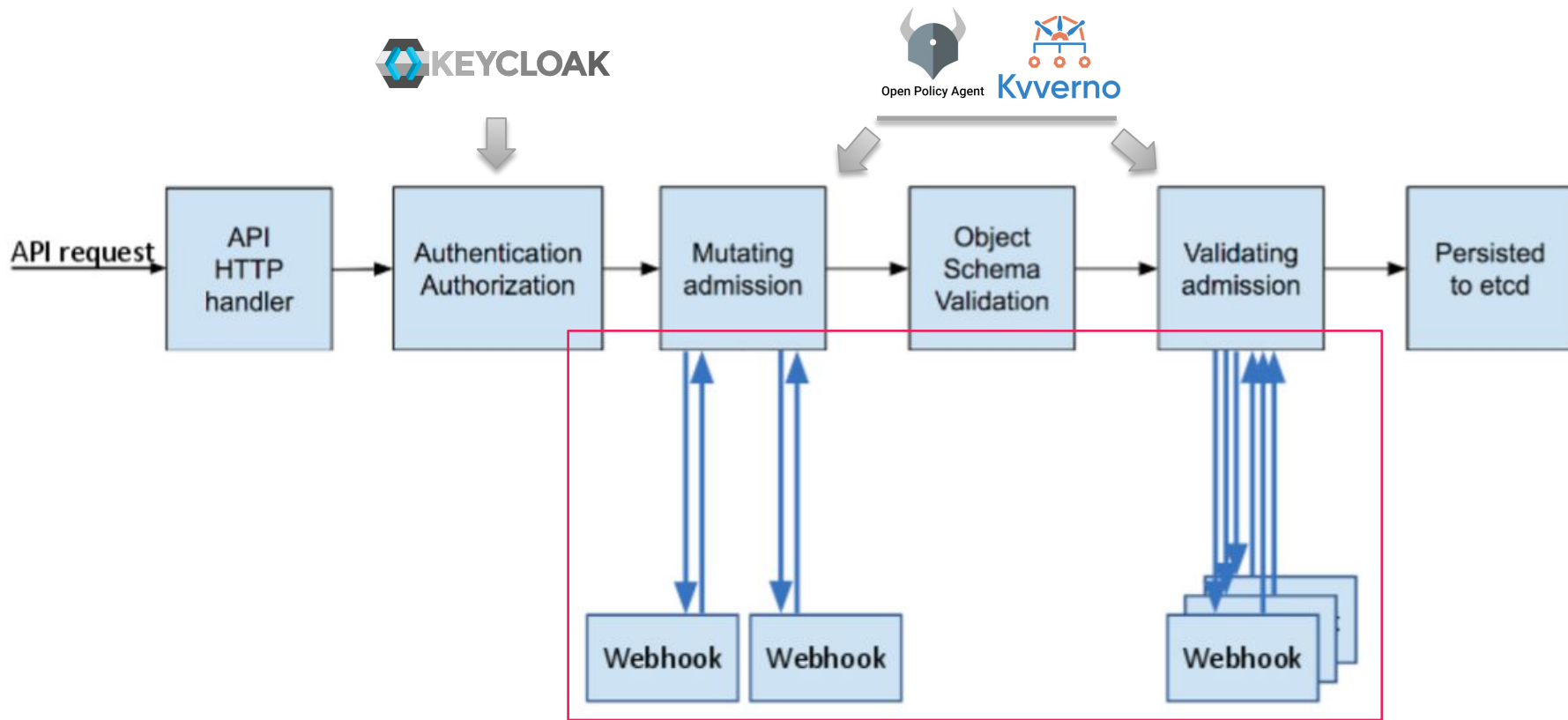
OpenInfra Days
Korea 2025

PART I

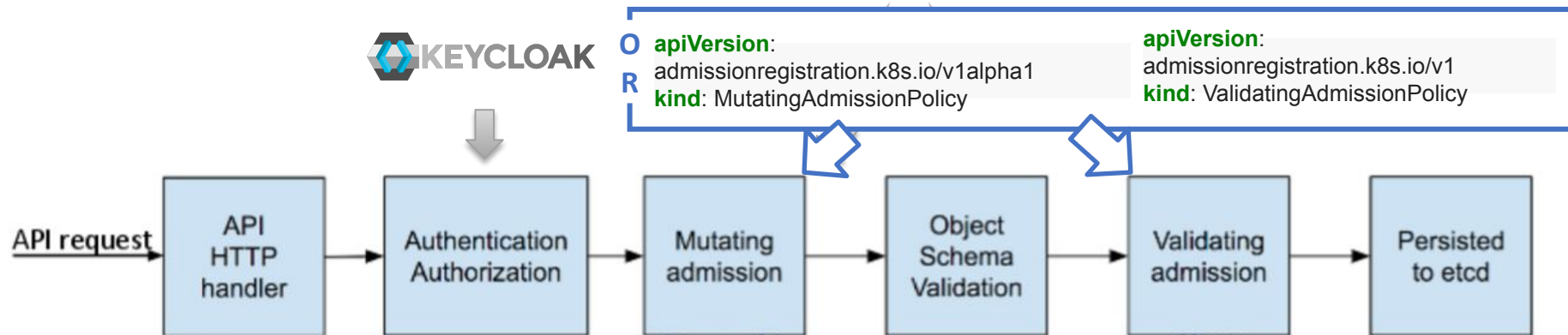
PaC: 과거



과거: Admission-Controllers



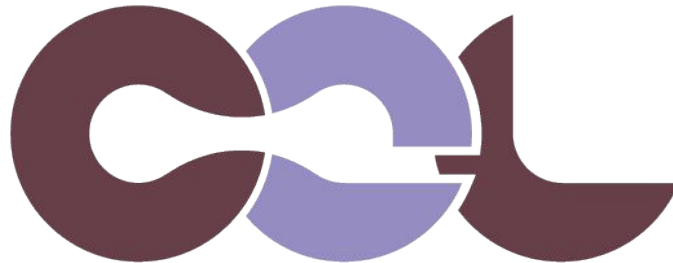
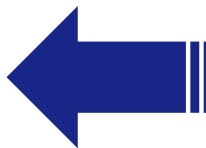
바뀐 : Admission-Controllers (웹훅이 없어도 동작 가능)



언어는 CEL(Common Expression Language)

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

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



COMMON EXPRESSION LANGUAGE

CEL이 쿠버네티스에 적용되기 까지 과정



변경 사항

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 / MutatingAdmissionPolicy, Alpha)
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_oWm4kV
 - Primary contact (assignee): [@cici37](#)
 - Responsible SIGs: sig-api-machinery
 - Enhancement target (which target equals to which milestone):
 - Alpha release target (x.y): 1.28
 - Beta release target (x.y): 1.29
 - 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/1x9RNaayvY00gXh1r1y50QFb11x8QWnk2v3XndkT5Y/e/d#bookmarkid.55kd8uoz25p5>
 - Primary contact (assignee): [@talclair](#)
 - Responsible SIGs: api-machinery
 - Enhancement target (which target equals to which milestone):
 - Alpha release target (x.y): 1.27
 - Beta release target (x.y): 1.28
 - Stable release target (x.y): 1.29

<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-ji](#)) [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 strict 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](#), [@eni](#))
- Promoted `AdmissionWebhookMatchConditions` to GA. The feature is now stable, and the feature gate is now locked to default. ([#123560](#), [@velichkovich](#))



OpenInfra
DAYS



KOREA

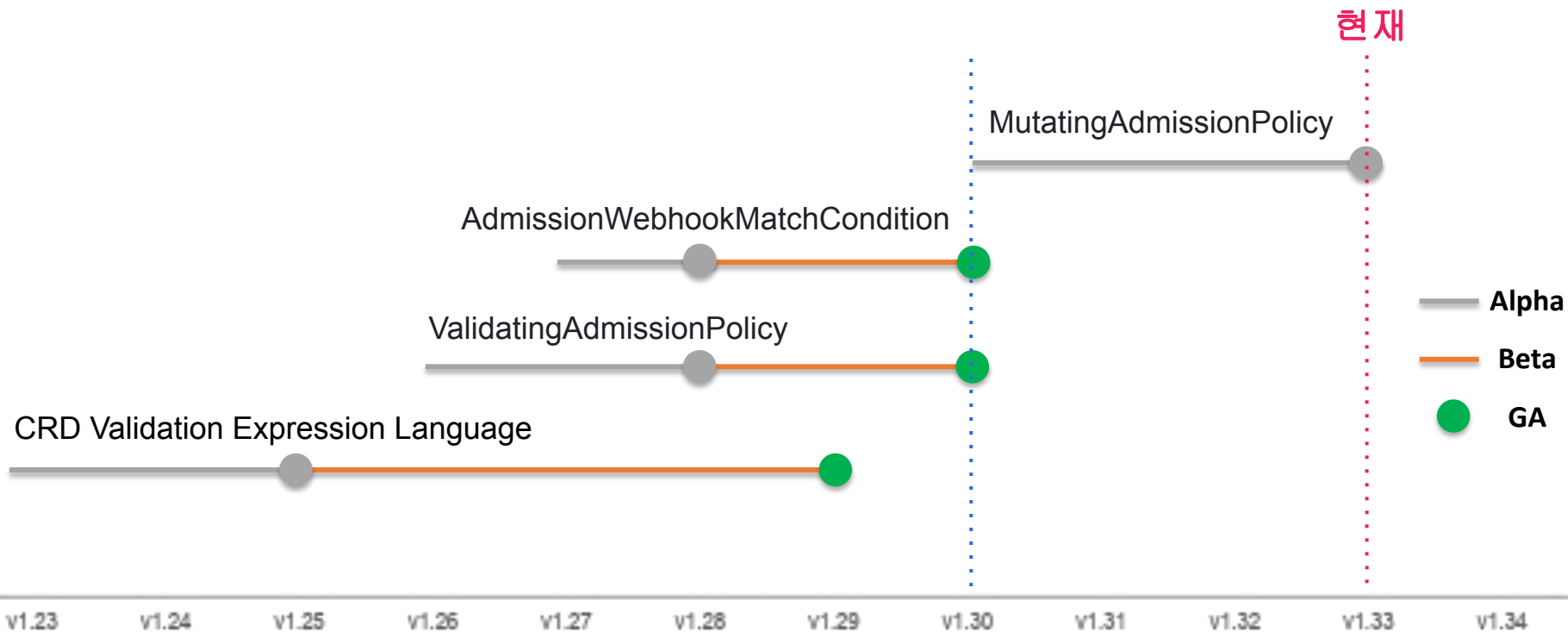
OpenInfra Days
Korea 2025

PART II

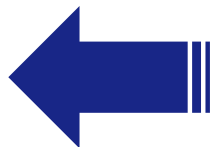
PaC: 현재



성숙도: CEL & Admission

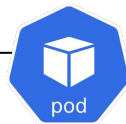


Policy as Code (PaC) ← 쿠버네티스의 CEL



```
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



```
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"
```

```
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



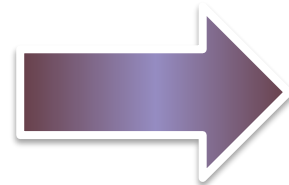
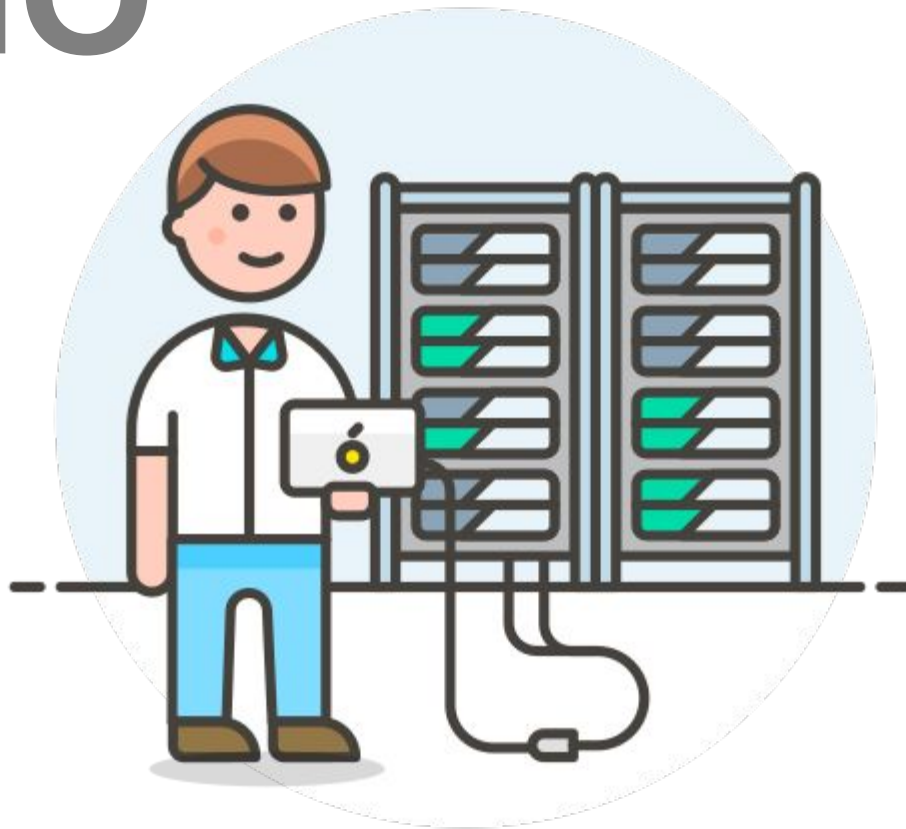
```
...  
matchConditions:  
- name: does-not-already-have-sidecar  
  expression: "!object.spec.initContainers.exists(ic,  
    ic.name == \"mesh-proxy\")"
```

Validation



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

DEMO



OpenInfra
DAYS



KOREA

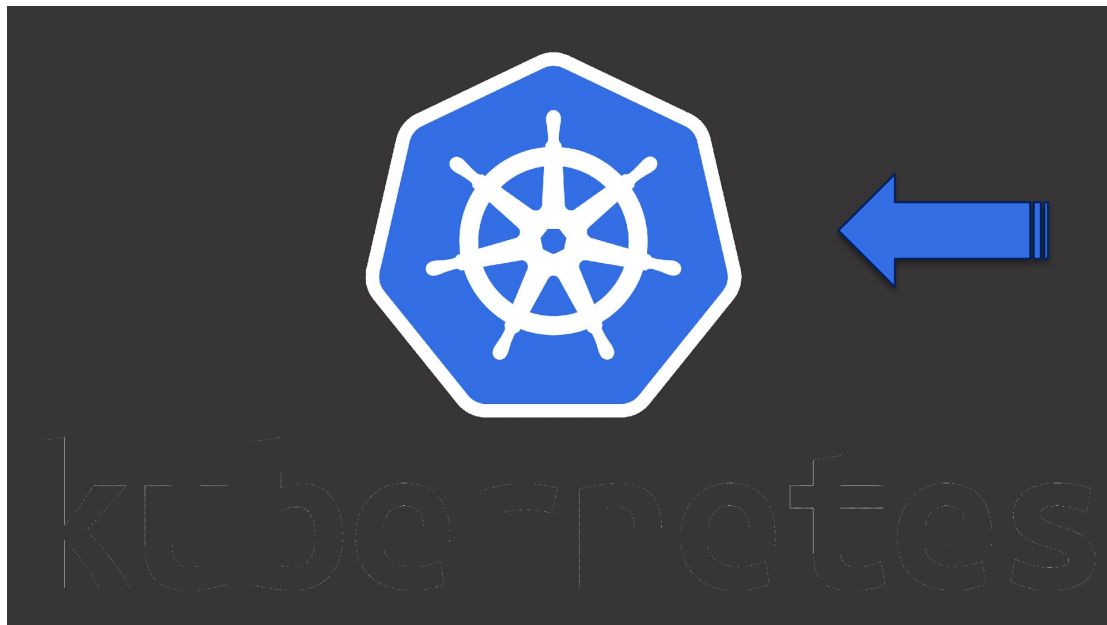
OpenInfra Days
Korea 2025

PART III

PaC: 미래



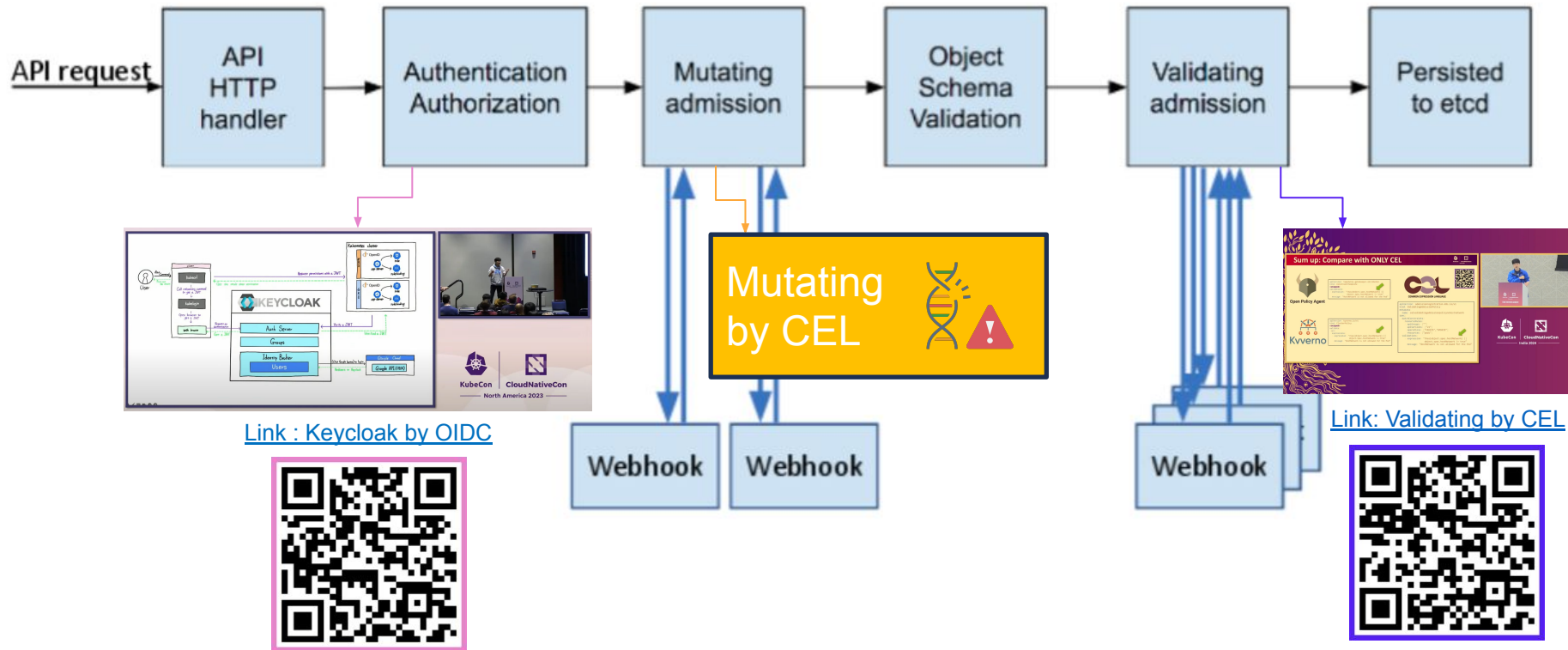
CEL은 이미 쿠버네티스에 적용됨



이제 곧 무언가가 더 쿠버네티스로 들어옵니다!

O **apiVersion:**
admissionregistration.k8s.io/v1alpha1
R **kind:** MutatingAdmissionPolicy

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



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/>