Kubernetes Community Days
MUNICH 2023

SPONSORS

metalstack cloud
ELASTICBRAINS
APE FACTORY
QA|WARE
Google Cloud
Grafana Labs
AppsCode
mkdev
ISOVALENT
camp tocamp
StormForge
okteto
lumigo
EXOSCALE
Red Hat
SysEleven
REPLY LIQUID
white duck
blueshoe

Speaker: Koray Oksay
Company: Kubermatic

Securing Your Kubernetes Workloads with Kyverno

koray@kubermatic.com

@korayoksay

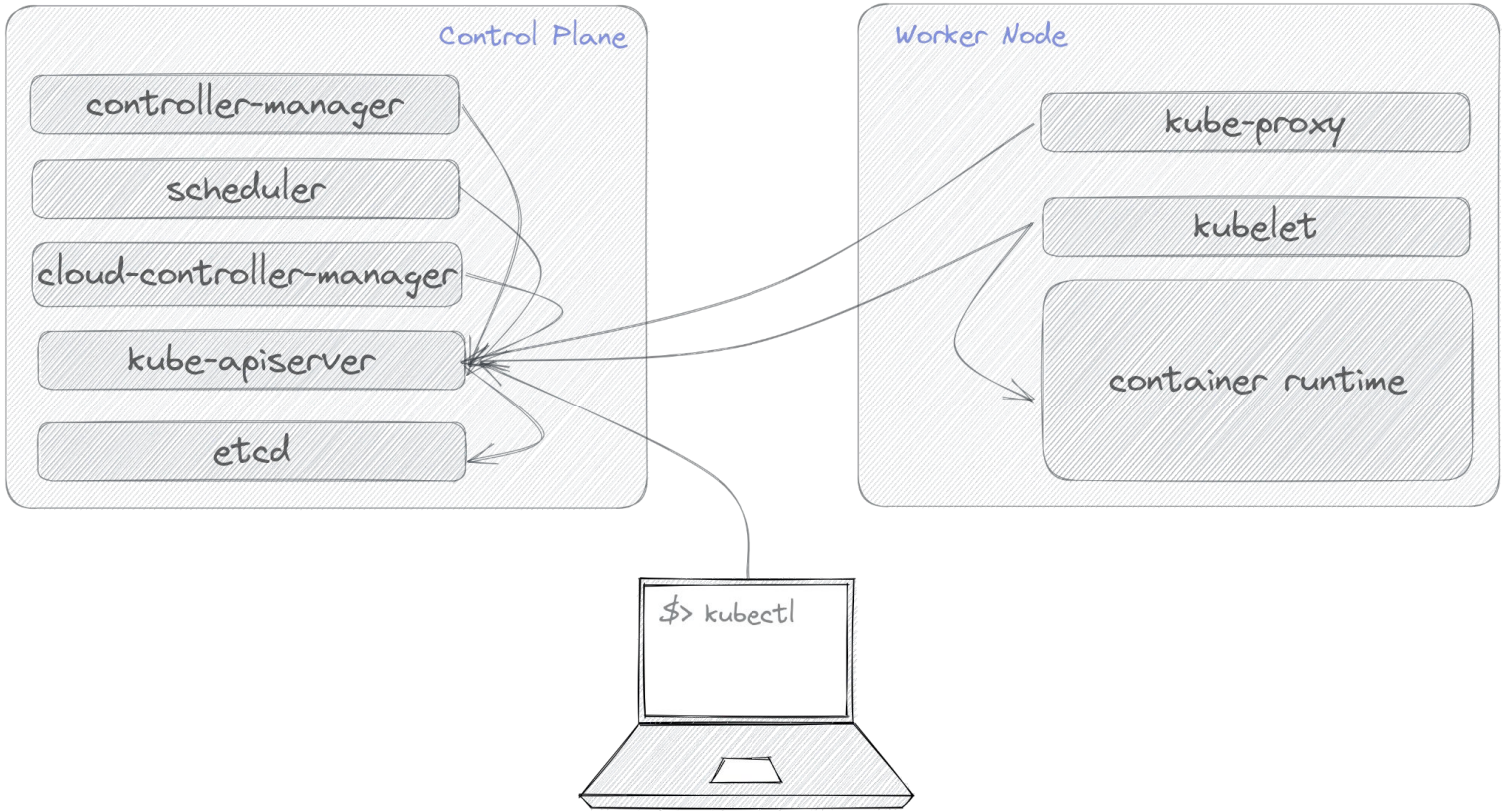
linkedin.com/in/korayoksay/

koksay

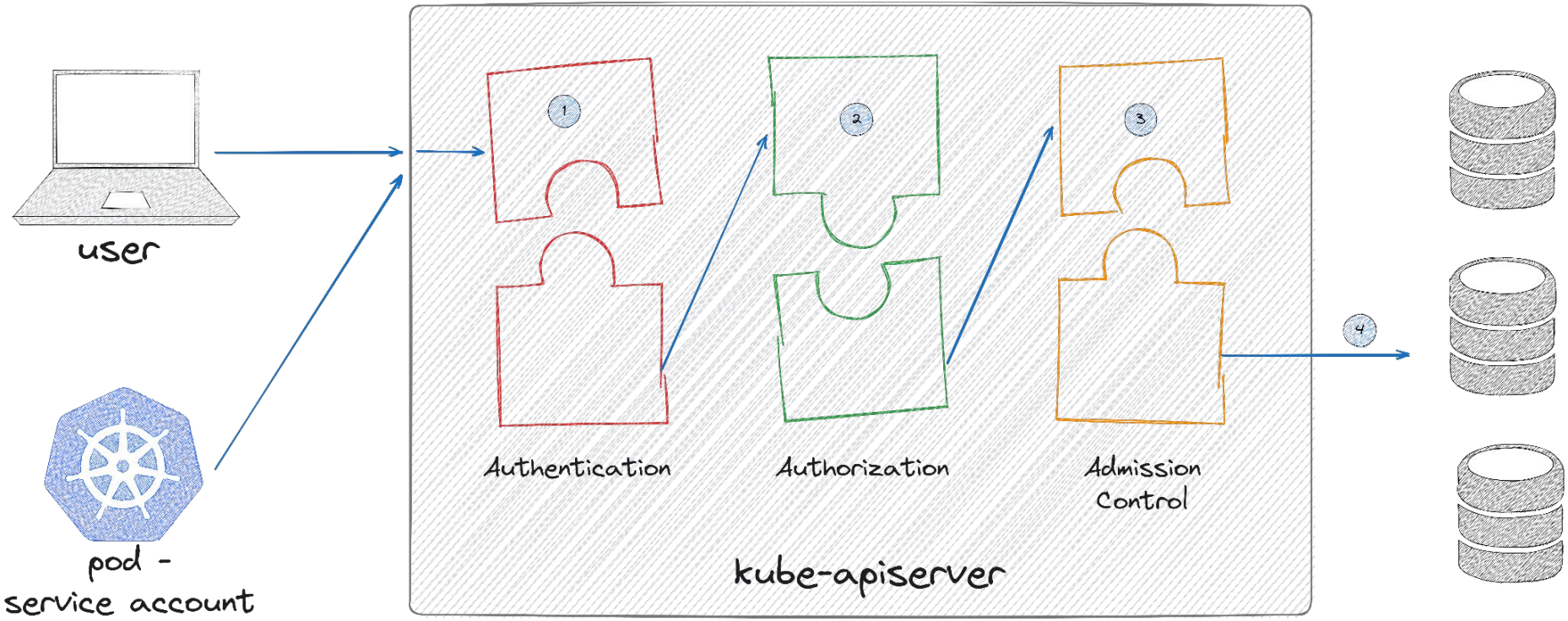
Who am I?

- Kubernetes Consultant & Instructor
- Working remotely from Istanbul
- Interested in Linux, Kubernetes, and cloud technologies
- CKA | CKAD | CKS | RHCE
- Linux Foundation Instructor for CK.*

Kubernetes Architecture



Access Control on the Kubernetes API



Admission Controllers

- Compiled-in Admission Plugins
  - DefaultStorageClass
  - LimitRanger
  - NamespaceLifeCycle
  - ...
- Dynamic Admission Control
  - Validating Admission Webhook
  - Mutating Admission Webhook

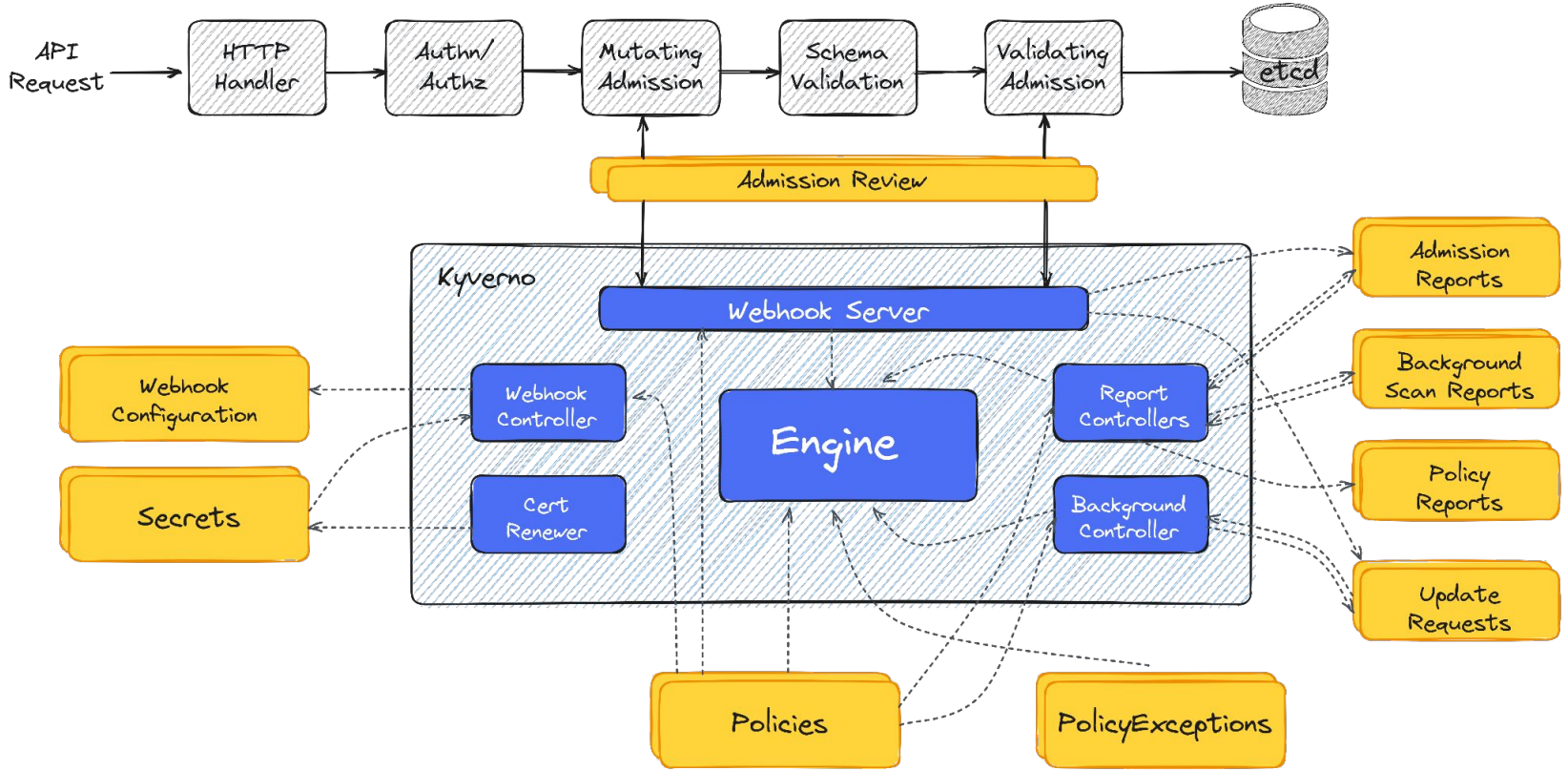
What is Kyverno?

- Greek for "Govern"
- Policies as Kubernetes resources (no new language to learn!)
- Validate, mutate, generate, or cleanup (remove) any resource
- Verify container images for software supply chain security

What is Kyverno?

- Inspect image metadata
- Synchronize configurations across Namespaces
- Test policies and validate resources using the Kyverno CLI, in your CI/CD pipeline, before applying to your cluster

High-Level Architecture



```yaml
## https://github.com/kyverno/kyverno/blob/main/charts/kyverno/values.yaml

  # -- Defines the `namespaceSelector` in the webhook configurations.
  # Note that it takes a list of `namespaceSelector` and/or `objectSelector` in the JSON format and only the first element
  # will be forwarded to the webhook configurations.
  # The Kyverno namespace is excluded if `excludeKyvernoNamespace` is `true` (default)
  webhooks: []
    # Exclude namespaces
    - namespaceSelector:
        matchExpressions:
        - key: kubernetes.io/metadata.name
          operator: NotIn
          values:
            - kube-system
            - kyverno
    # Exclude objects
    # - objectSelector:
    #     matchExpressions:
    #     - key: webhooks.kyverno.io/exclude
    #       operator: DoesNotExist
```

```yaml
apiVersion: kyverno.io/v1
kind: ClusterPolicy
metadata:
  name: disallow-privileged-containers
spec:
  validationFailureAction: audit
  background: true
  rules:
    - name: privileged-containers
      match:
        any:
        - resources:
            kinds:
              - Pod
      validate:
        message: >-
          Privileged mode is disallowed. The fields spec.containers[*].securityContext.privileged
          and spec.initContainers[*].securityContext.privileged must be unset or set to `false`.
        pattern:
          spec:
            =(ephemeralContainers):
              - =(securityContext):
                  =(privileged): "false"
            =(initContainers):
              - =(securityContext):
                  =(privileged): "false"
            containers:
              - =(securityContext):
                  =(privileged): "false"
```

```yaml
apiVersion: kyverno.io/v1
kind: ClusterPolicy
metadata:
  name: block-stale-images
spec:
  validationFailureAction: audit
  rules:
    - name: block-stale-images
      match:
        any:
        - resources:
            kinds:
            - Pod
      validate:
        message: "Images built more than 6 months ago are prohibited."
        foreach:
        - list: "request.object.spec.containers"
          context:
          - name: imageData
            imageRegistry:
              reference: "{{ element.image }}"
          deny:
            conditions:
              all:
                - key: "{{ time_since('', '{{ imageData.configData.created }}', '') }}"
                  operator: GreaterThan
                  value: 4380h
```

KUBERMATIC

>_ DEMO

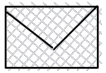
https://killercoda.com/kyverno-demo/course/kyverno

KUBERMATIC

QUESTIONS?

KUBERMATIC

THANK YOU!



koray@kubermatic.com

@korayoksay

linkedin.com/in/korayoksay/

koksay