Headless & API date | Liferay | mia Platform | Intesys | SESSIONE TECH

Secure GitOps su Kubernetes: come evolvere in sicurezza il motore delle nostre API

ENRICO COSTANZI
SOFTWARE DEVELOPER, INTESYS

Agenda

1. Perché GitOps?
2. Kubernetes GitOps
3. Secure Kubernetes GitOps Pipeline

Headless & API date

SESSIONE TECH

GitOps

Intesys.it

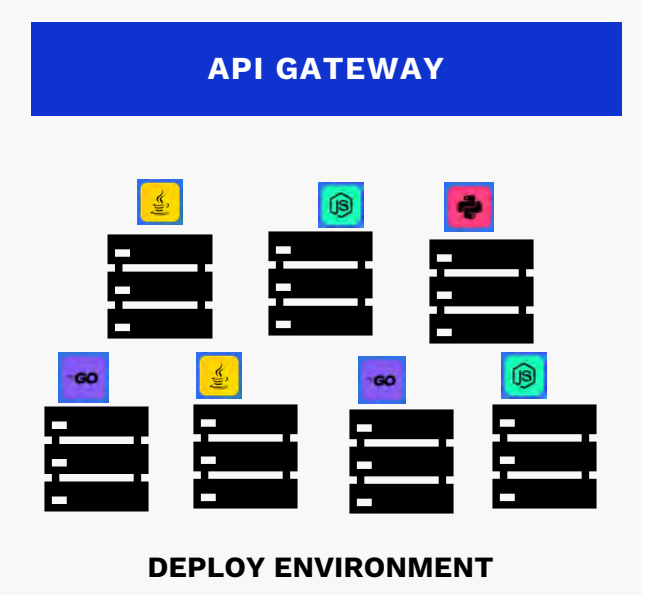
“**DevOps** is a set of **practices**, **tools**, and a **cultural philosophy** that automate and integrate the processes between **software development** and IT teams.

It emphasizes team empowerment, cross-team **communication** and **collaboration**, and technology **automation**.”

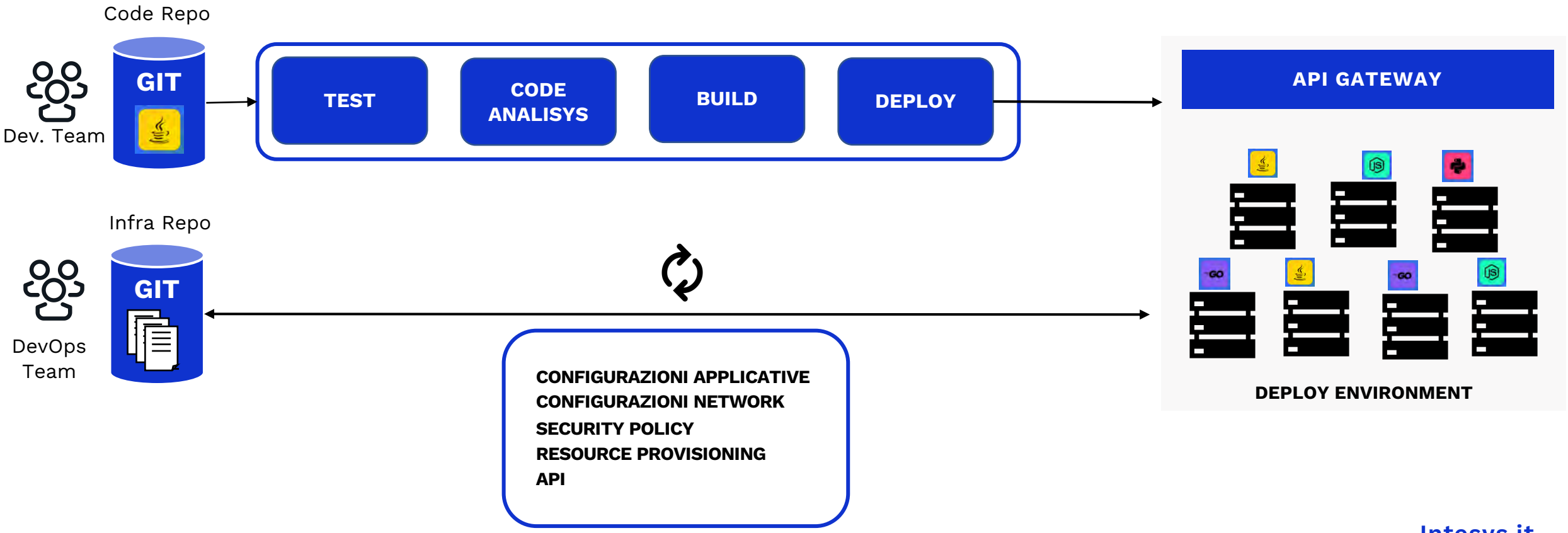
www.atlassian.com/devops

Non solo deploy applicativi

- Configurazioni Applicative
- Configurazioni Network
- Policy
- API (throttling, rate limiting)
- Resource Provisioning



Infrastructure as Code?



GitOps

Approccio Dichiarativo

L’architettura può essere descritta in modo dichiarativo.

X as Code

Git *Single Source of Truth.* (Infrastructure as Code, Network as Code, Policies as Code).

Automazione

Le modifiche alle configurazioni vengono applicate in automatico all’infrastruttura.

Collaborazione

Le modifiche alle configurazioni avvengono in modo collaborativo. (Code Review & Pull Requests).

Headless & API date

SESSIONE TECH

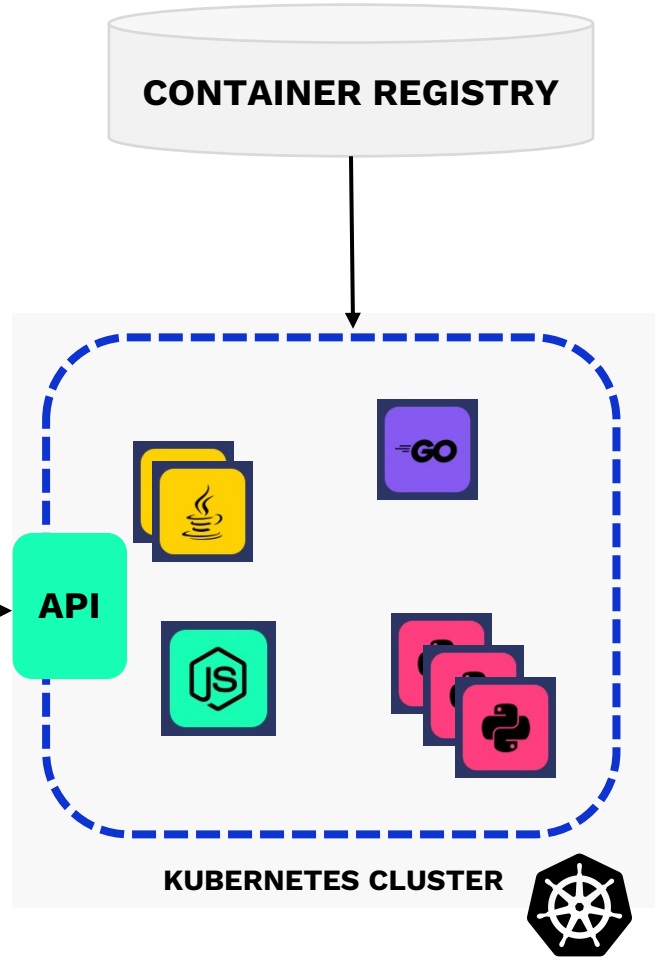
GitOps & Kubernetes

Intesys.it

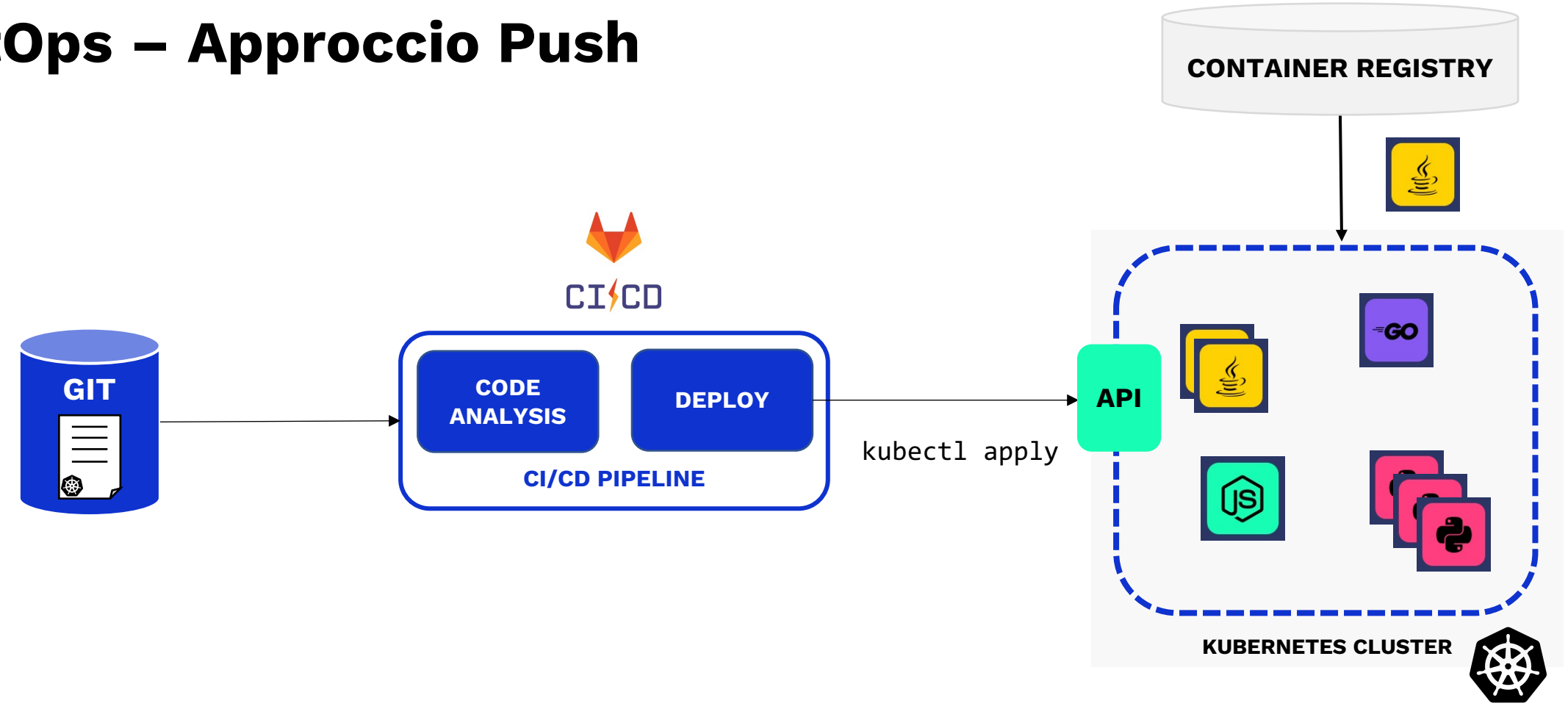
Kubernetes Declarative Management

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: pdf-service
spec:
  replicas: 1 2
  selector:
    matchLabels:
      app: pdf-service
  template:
    metadata:
      labels:
        app: pdf-service
    spec:
      containers:
        - name: app
          image: docker.intesys.it/k8slab/pdf-service
          readinessProbe:
            httpGet:
              path: /management/health/readiness
              port: 8080
          livenessProbe:
            httpGet:
              path: /management/health/liveness
              port: 8080

      imagePullSecrets:
        - name: docker-intesys
```

kubectl apply



GitOps – Approccio Push



passed **Pipeline #60194** triggered 2 days ago by Enrico Costanzi

Delete

Update pdf-service probes

2 jobs for develop in 13 minutes and 26 seconds (queued for 6 seconds)

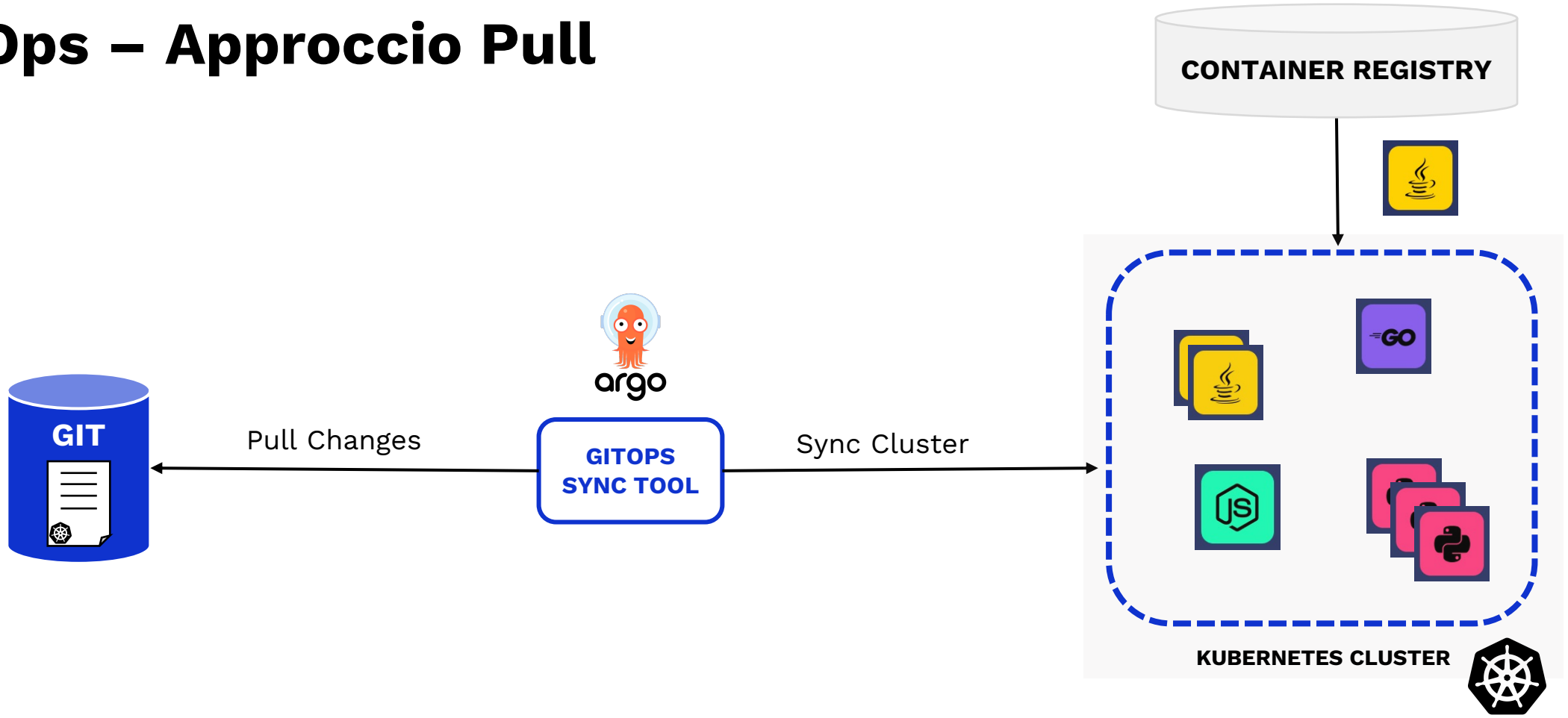
53c9cb7c

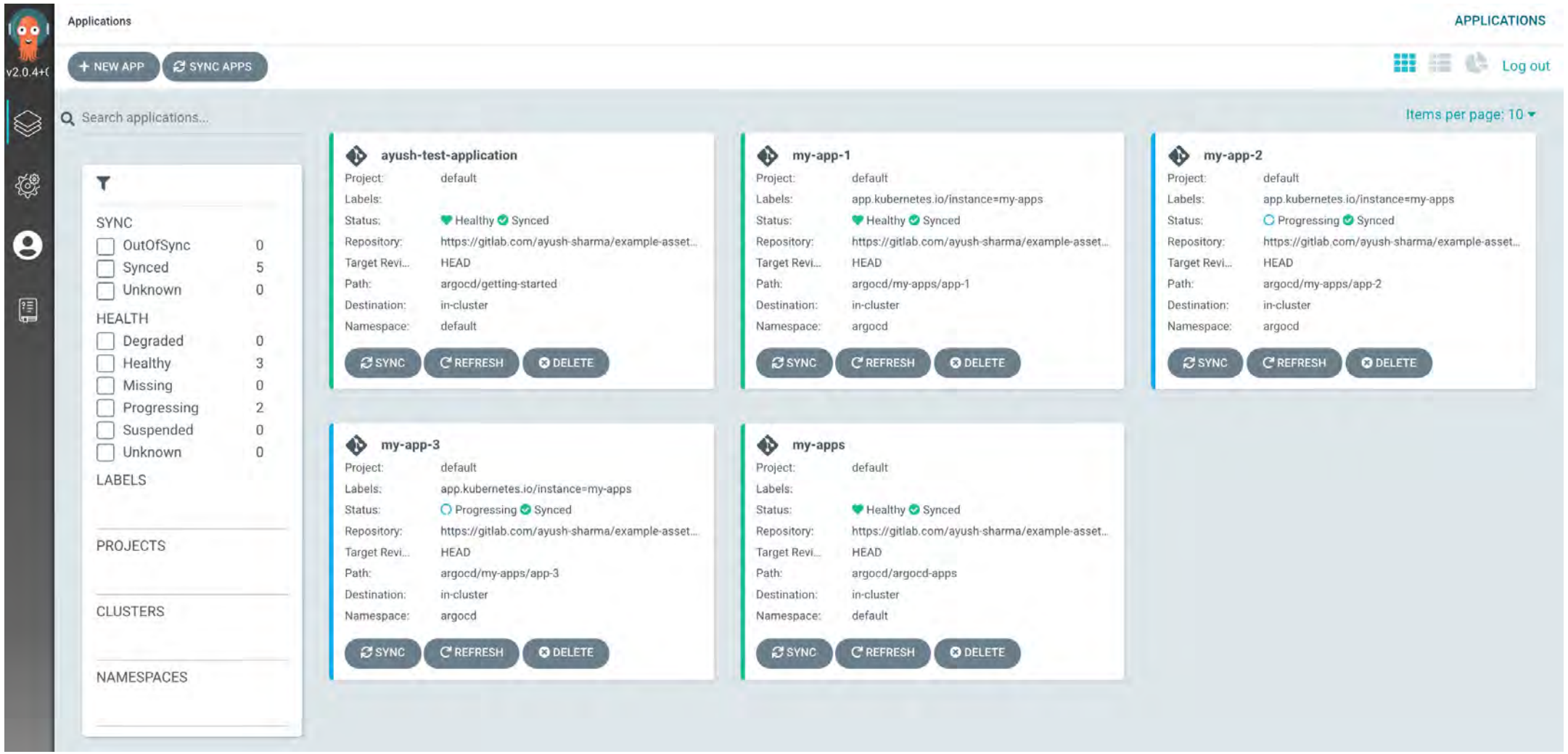
No related merge requests found.

Pipeline | Needs | Jobs 2

Test	Analyze
config-check	k8s-deploy

GitOps – Approccio Pull



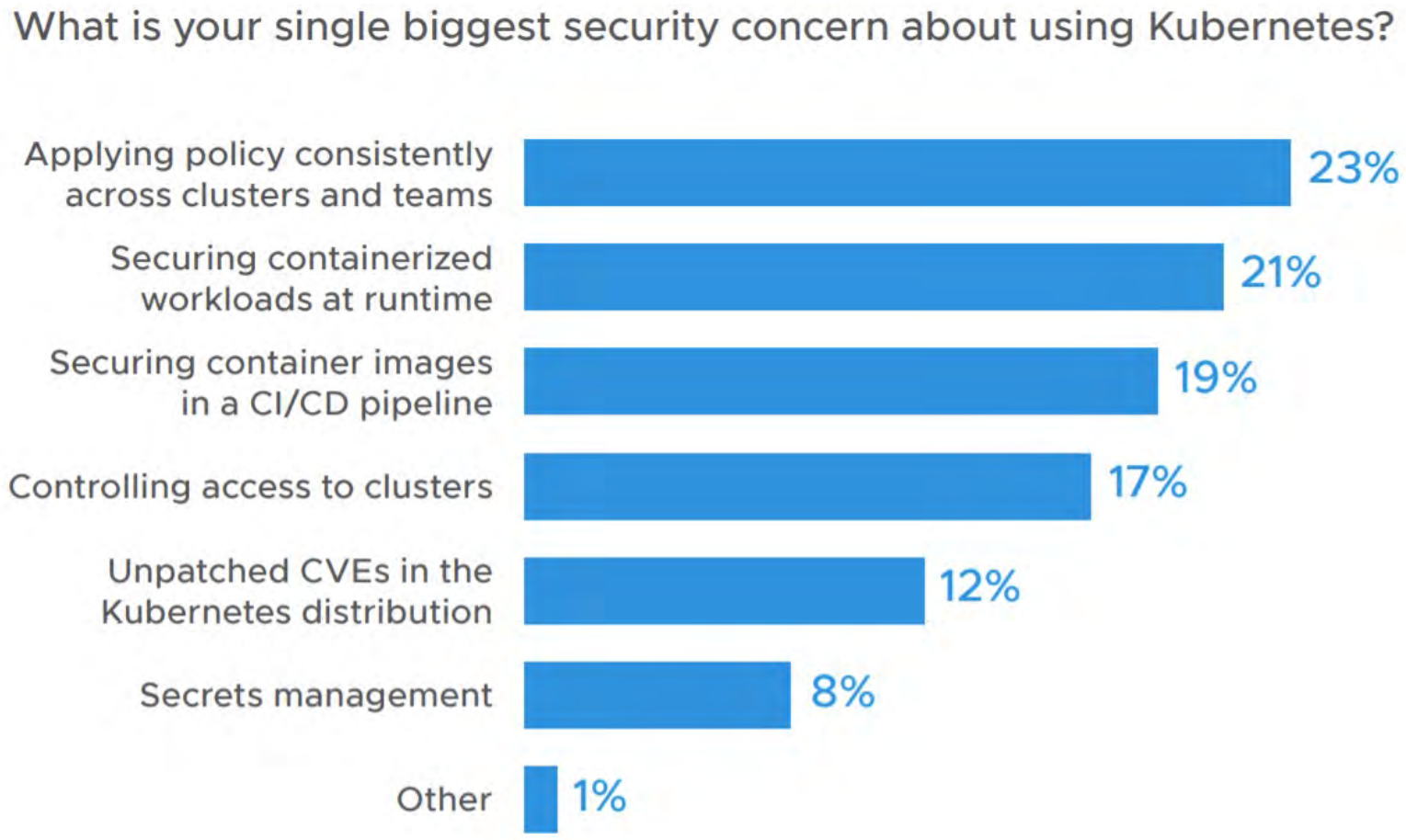

Applications
APPLICATIONS
+ NEW APP
SYNC APPS
Log out
Search applications...
Items per page: 10
SYNC
OutOfSync 0
Synced 5
Unknown 0
HEALTH
Degraded 0
Healthy 3
Missing 0
Progressing 2
Suspended 0
Unknown 0
LABELS
PROJECTS
CLUSTERS
NAMESPACES
ayush-test-application
Project: default
Labels:
Status: Healthy Synced
Repository: https://gitlab.com/ayush-sharma/example-asset...
Target Revi... HEAD
Path: argocd/getting-started
Destination: in-cluster
Namespace: default
SYNC REFRESH DELETE
my-app-1
Project: default
Labels: app.kubernetes.io/instance=my-apps
Status: Healthy Synced
Repository: https://gitlab.com/ayush-sharma/example-asset...
Target Revi... HEAD
Path: argocd/my-apps/app-1
Destination: in-cluster
Namespace: argocd
SYNC REFRESH DELETE
my-app-2
Project: default
Labels: app.kubernetes.io/instance=my-apps
Status: Progressing Synced
Repository: https://gitlab.com/ayush-sharma/example-asset...
Target Revi... HEAD
Path: argocd/my-apps/app-2
Destination: in-cluster
Namespace: argocd
SYNC REFRESH DELETE
my-app-3
Project: default
Labels: app.kubernetes.io/instance=my-apps
Status: Progressing Synced
Repository: https://gitlab.com/ayush-sharma/example-asset...
Target Revi... HEAD
Path: argocd/my-apps/app-3
Destination: in-cluster
Namespace: argocd
SYNC REFRESH DELETE
my-apps
Project: default
Labels:
Status: Healthy Synced
Repository: https://gitlab.com/ayush-sharma/example-asset...
Target Revi... HEAD
Path: argocd/argocd-apps
Destination: in-cluster
Namespace: default
SYNC REFRESH DELETE

Headless & API date

SESSIONE TECH

Kubernetes Security

Intesys.it

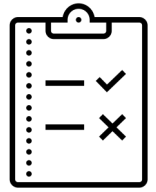


The State of Kubernetes 2021 – by VMWare

Strumenti per un GitOps sicuro

CONTAINER REGISTRY

CONFIGURATIONS CODE ANALYSIS



POLICY MANAGER

Strumenti per un GitOps sicuro

CONTAINER REGISTRY

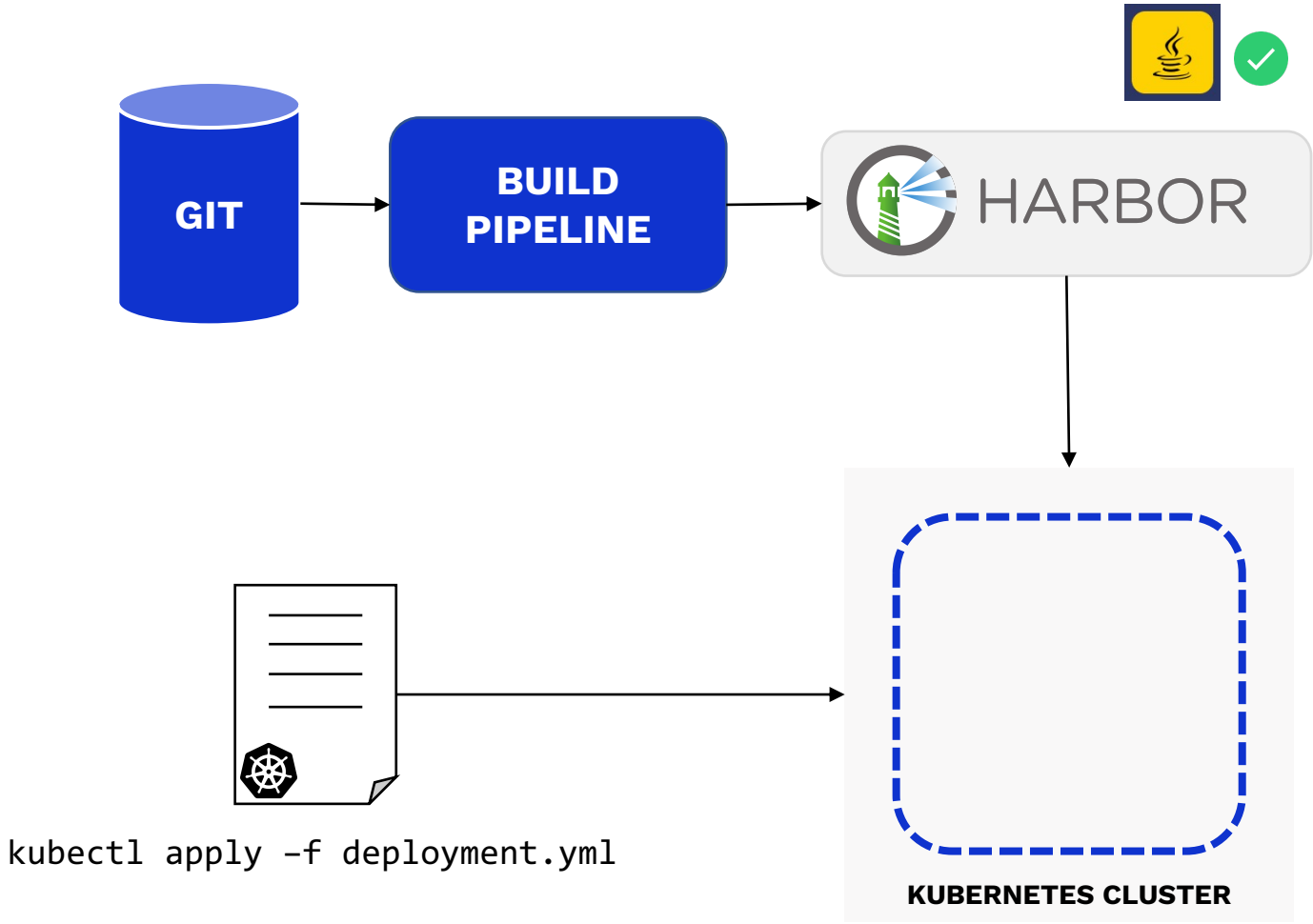
CONFIGURATIONS CODE ANALYSIS

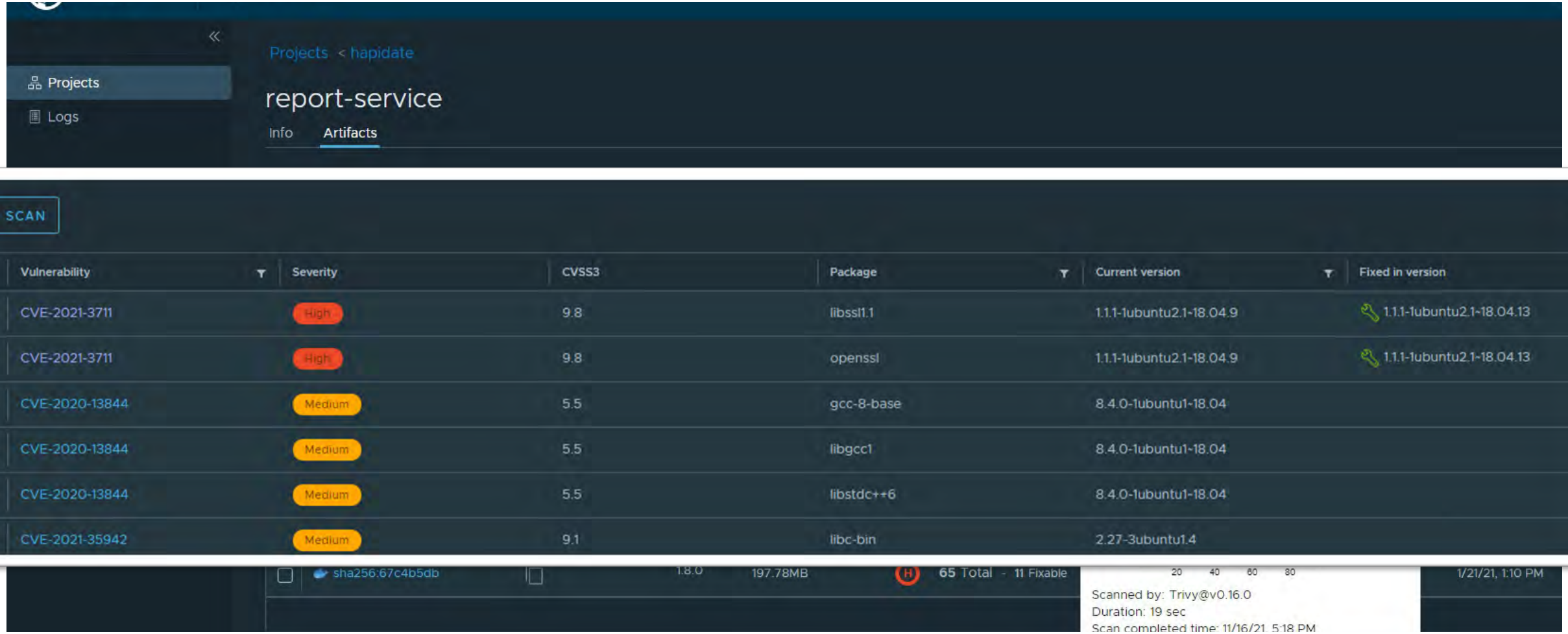
POLICY MANAGER

Harbor

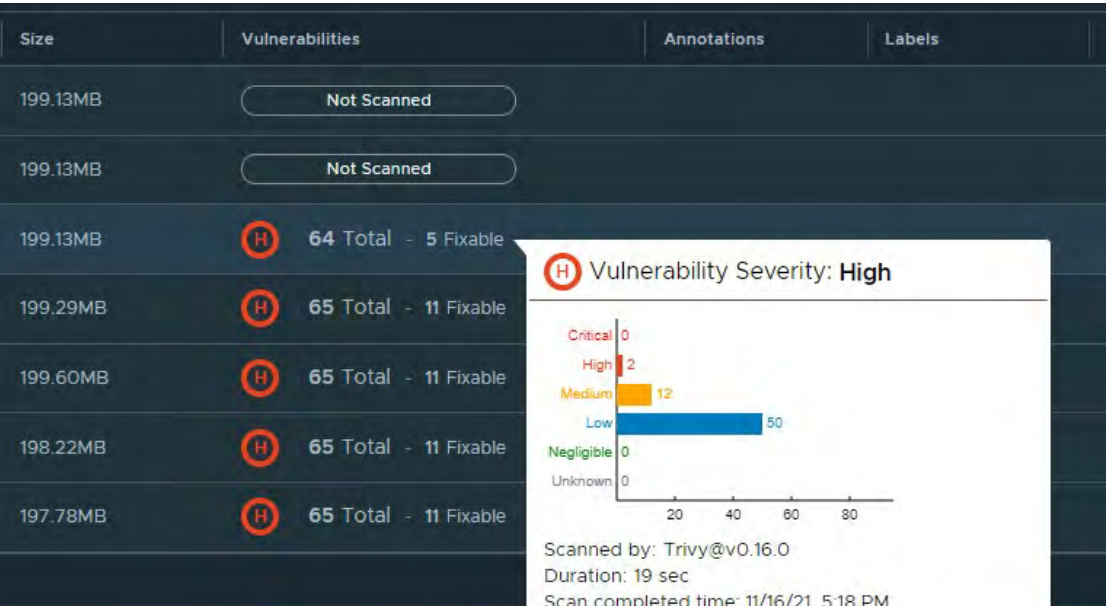
Cloud Native Container Registry

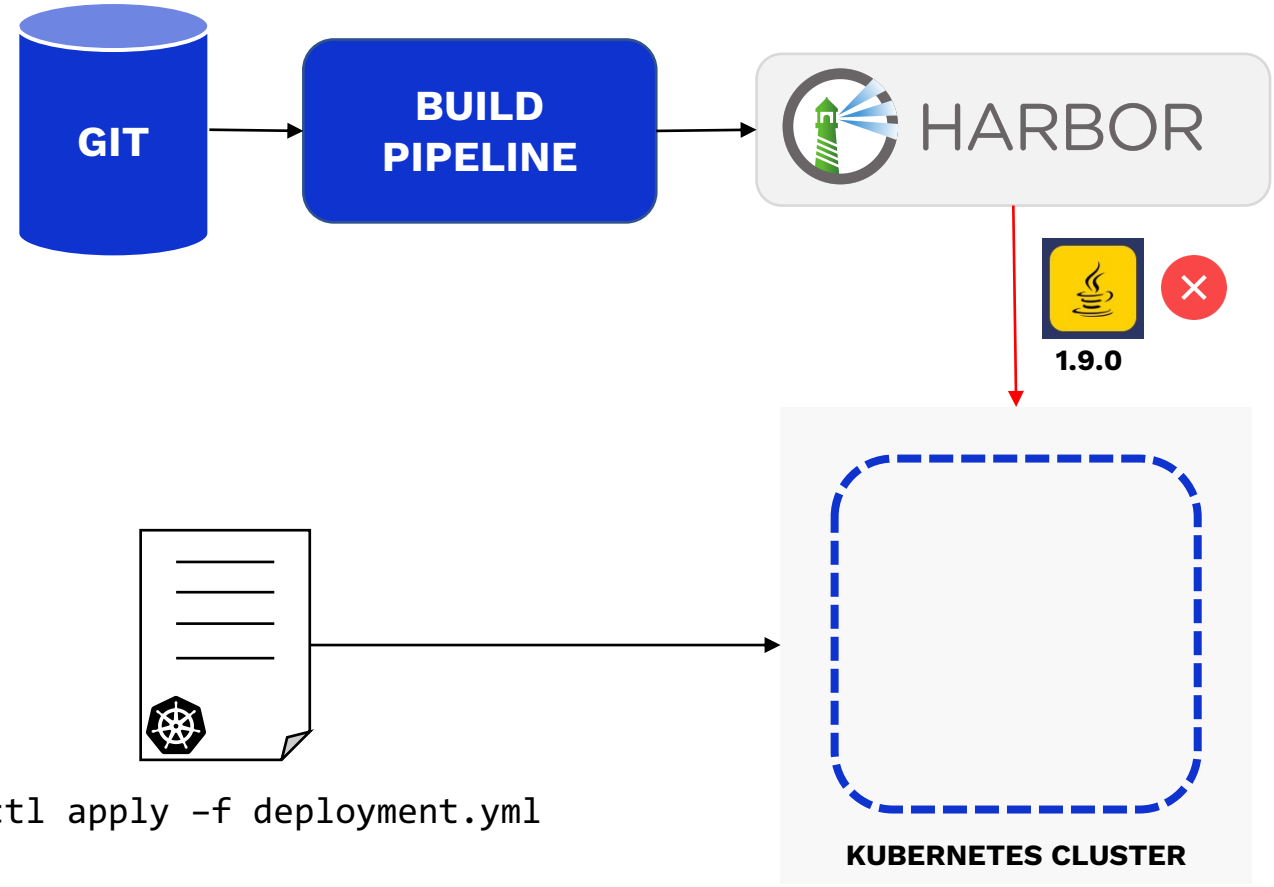
- Image Vulnerability Scanning
- Content Trust
- Tag Immutability
- Metriche




Projects
Logs
Projects < hapidate
report-service
Info
Artifacts
SCAN
Vulnerability
Severity
CVSS3
Package
Current version
Fixed in version
CVE-2021-3711
High
9.8
libssl1.1
1.1.1-1ubuntu2.1~18.04.9
1.1.1-1ubuntu2.1~18.04.13
CVE-2021-3711
High
9.8
openssl
1.1.1-1ubuntu2.1~18.04.9
1.1.1-1ubuntu2.1~18.04.13
CVE-2020-13844
Medium
5.5
gcc-8-base
8.4.0-1ubuntu1~18.04
CVE-2020-13844
Medium
5.5
libgcc1
8.4.0-1ubuntu1~18.04
CVE-2020-13844
Medium
5.5
libstdc++6
8.4.0-1ubuntu1~18.04
CVE-2021-35942
Medium
9.1
libc-bin
2.27-3ubuntu1.4
sha256:67c4b5db
1.8.0
197.78MB
65 Total
11 Fixable
20
40
60
80
Scanned by: Trivy@v0.16.0
Duration: 19 sec
Scan completed time: 11/16/21, 5:18 PM
1/21/21, 1:10 PM

Harbor






```
kubectl apply -f deployment.yml
```

Strumenti per un GitOps sicuro

CONTAINER REGISTRY

CONFIGURATIONS CODE ANALYSIS

POLICY MANAGER

KubeLinter

Analisi YML di Kubernetes

- Validazione YML
- Focus su security e produzione
- Integrabile in pipeline CI/CD


```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: pdf-service
spec:
  replicas: 1
  selector:
    matchLabels:
      app: pdf-service
  template:
    metadata:
      labels:
        app: pdf-service
    spec:
      containers:
        - name: app
          image: docker.intesys.it/k8slab/pdf-service
          # securityContext:
            # runAsNonRoot: true
            # readOnlyRootFilesystem: true
          env:
            - name: SPRING_DATASOURCE_URL
              value: jdbc:postgresql://postgres:5432/pdfservice
```

KubeLinter
esempio

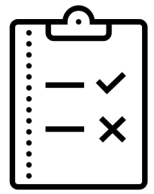
```
> kube-linter lint pdf-service/pdf-service-deploy.yaml --format plain
KubeLinter 0.2.5

pdf-service/pdf-service-deploy.yaml: (object: <no namespace>/pdf-service apps/v1, Kind=Deployment) container "app" does not have a read-only root file system (check: no-read-only-root-fs, remediation: Set readOnlyRootFilesystem to true in the container securityContext.)

pdf-service/pdf-service-deploy.yaml: (object: <no namespace>/pdf-service apps/v1, Kind=Deployment) container "app" is not set to runAsNonRoot (check: run-as-non-root, remediation: Set runAsUser to a non-zero number and runAsNonRoot to true in your pod or container securityContext. Refer to https://kubernetes.io/docs/tasks/configure-pod-container/security-context/ for details.)

Error: found 2 lint errors
```

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: pdf-service
spec:
  replicas: 1
  selector:
    matchLabels:
      app: pdf-service
  template:
    metadata:
      labels:
        app: pdf-service
    spec:
      containers:
        - name: app
          image: docker.intesys.it/k8slab/pdf-service
          # securityContext:
            # runAsNonRoot: true
            # readOnlyRootFilesystem: true
          env:
            - name: SPRING_DATASOURCE_URL
              value: jdbc:postgresql://postgres:5432/pdfservice
```

Strumenti per un GitOps sicuro

CONTAINER REGISTRY

CONFIGURATIONS CODE ANALYSIS



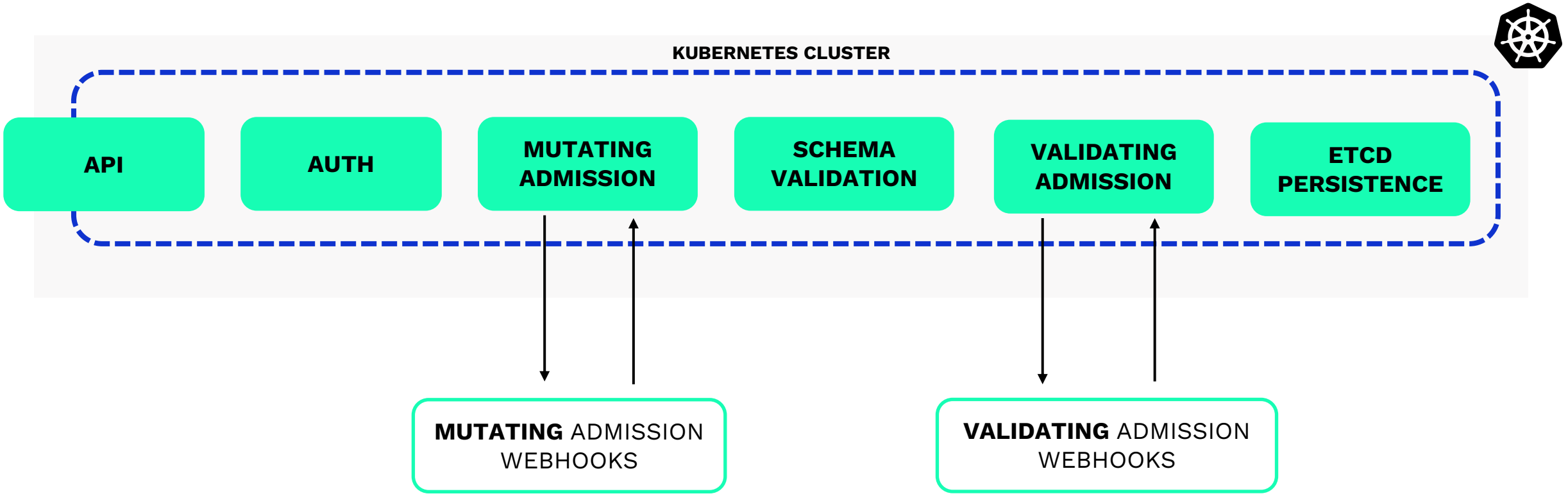
POLICY MANAGER

Kyverno

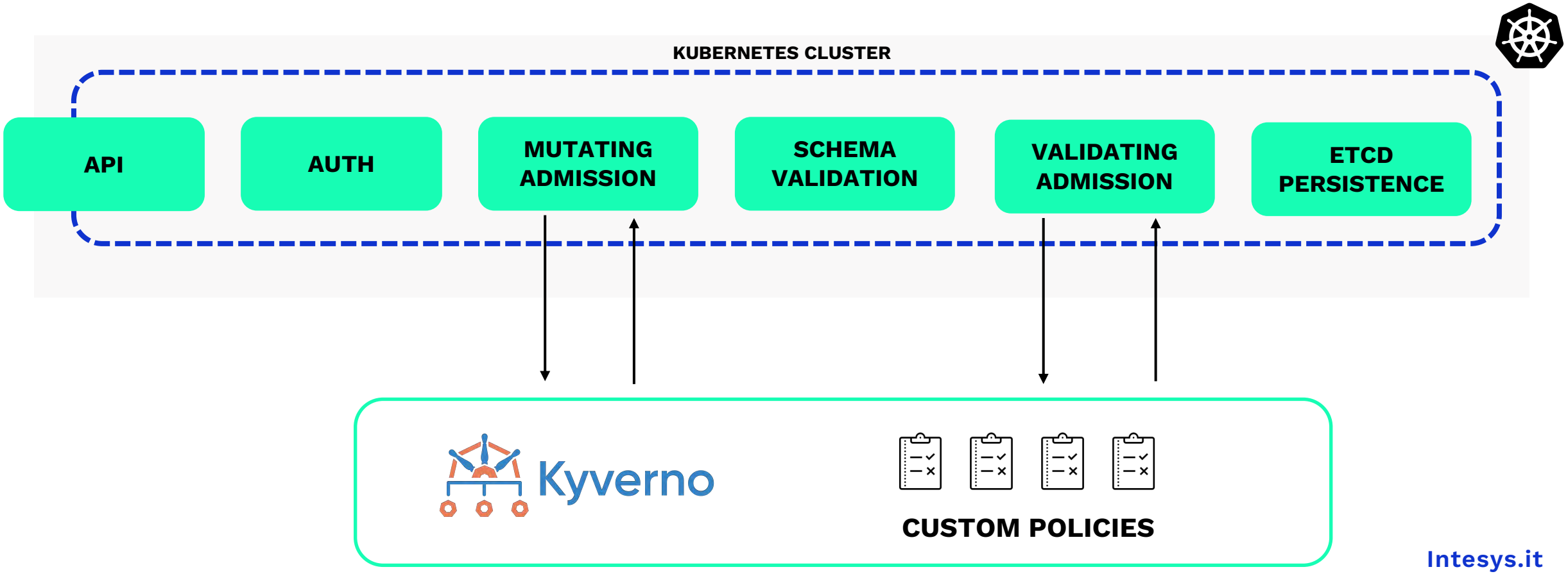
Policy Engine per Kubernetes

- Policy come Risorse Kubernetes
- Validazione, Modifica, Generazione Risorse
- Enforce vs Audit
- Reporting delle violazioni alle Policy
- Globali vs Namespace
- CLI per testing delle policy
- No programmazione

Kubernetes Admission Controllers



Kyverno – Dynamic Admission Controller



Esempio

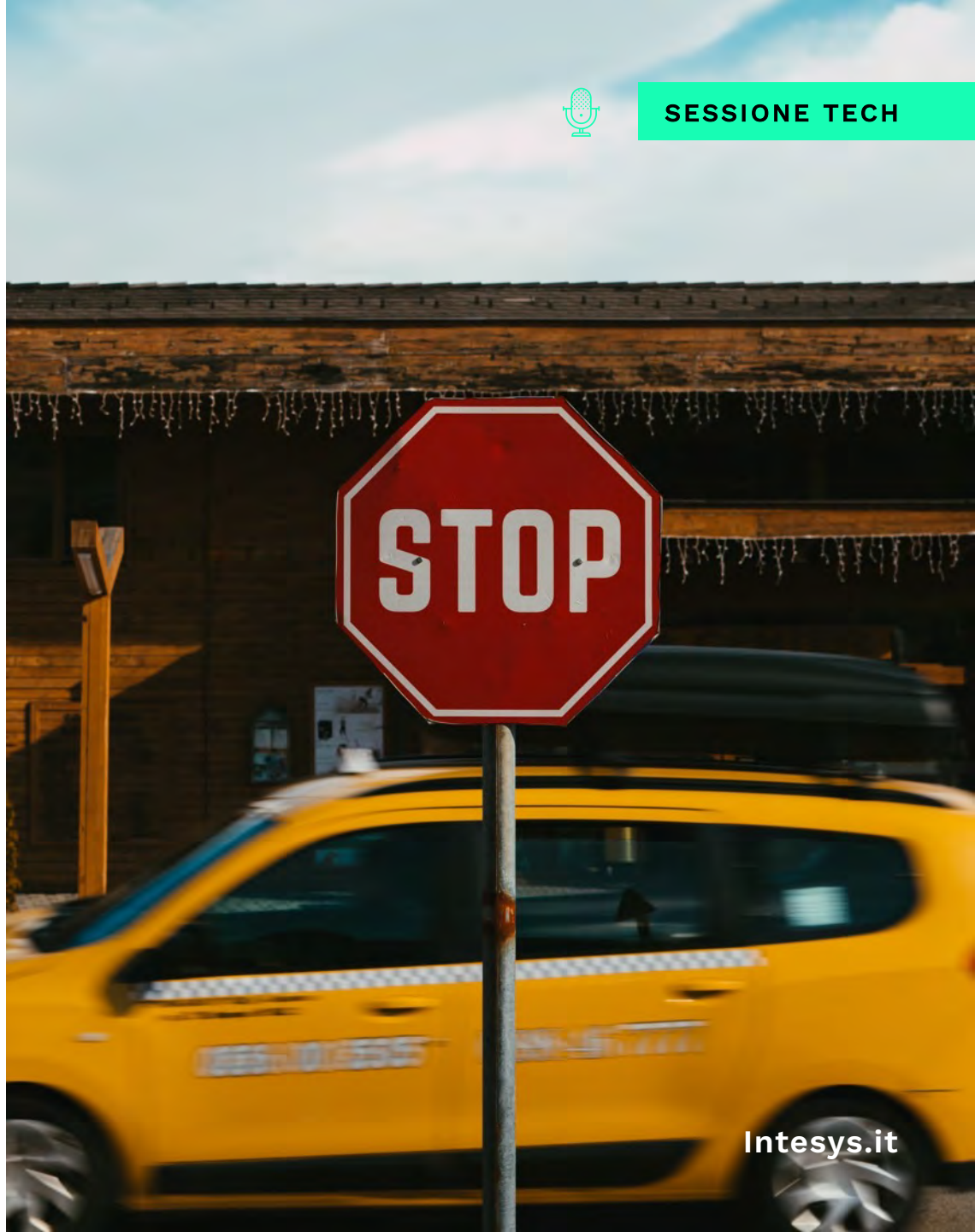
```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: pdf-service
spec:
  replicas: 1
  selector:
    matchLabels:
      app: pdf-service
  template:
    metadata:
      labels:
        app: pdf-service
    spec:
      containers:
        - name: docker-intesys
```

```yaml
apiVersion: kyverno.io/v1
kind: Policy
metadata:
  name: require-requests-limits
spec:
  validationFailureAction: enforce
  background: true
  rules:
  - name: validate-resources
    match:
      resources:
        kinds:
        - Deployment
    validate:
      message: "CPU and memory resource requests and limits are required."
      pattern:
```

```
> k apply -k pdf-service/
Error from server: error when creating "pdf-service/": admission webhook "validate.kyverno.svc-fail" denied the request:

resource Deployment/ecommercelab/pdf-service was blocked due to the following policies

require-requests-limits:
  validate-resources: 'validation error: CPU and memory resource requests and limits
    are required. Rule validate-resources failed at path /spec/template/spec/containers/0/resources/limits/'
```

Esempi di Policy

- Disallow “latest” tag
- Require Labels
- Require Pod Probes
- Restrict Image Registries
- Restrict External Ips
- Disallow Load Balancer
- Require Network Policy
- Block Updates and Deletes

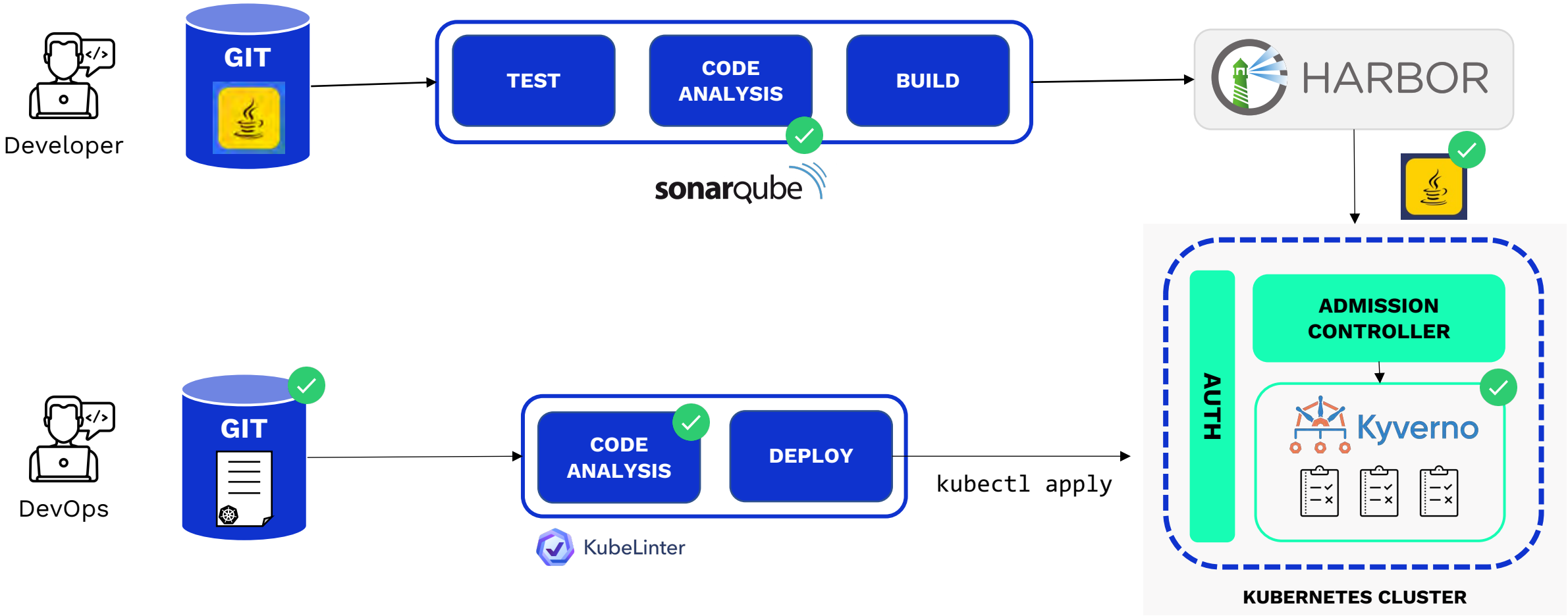


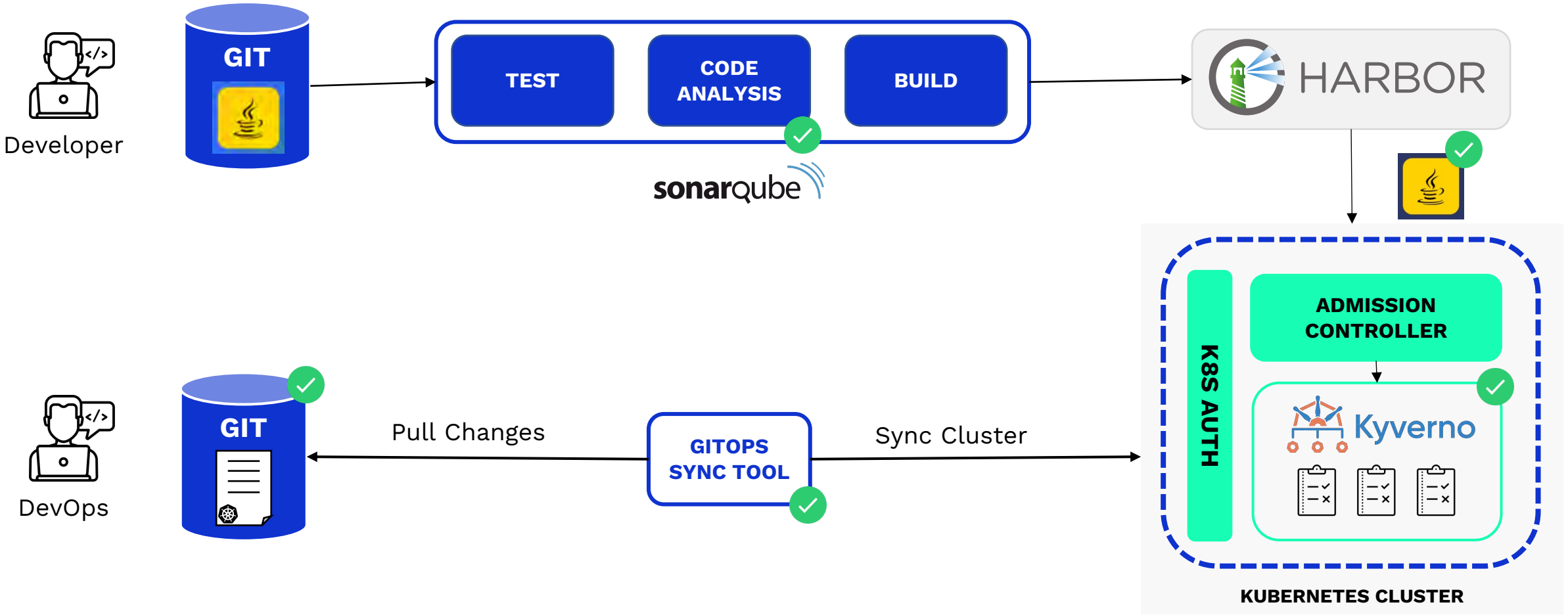
Headless & API date

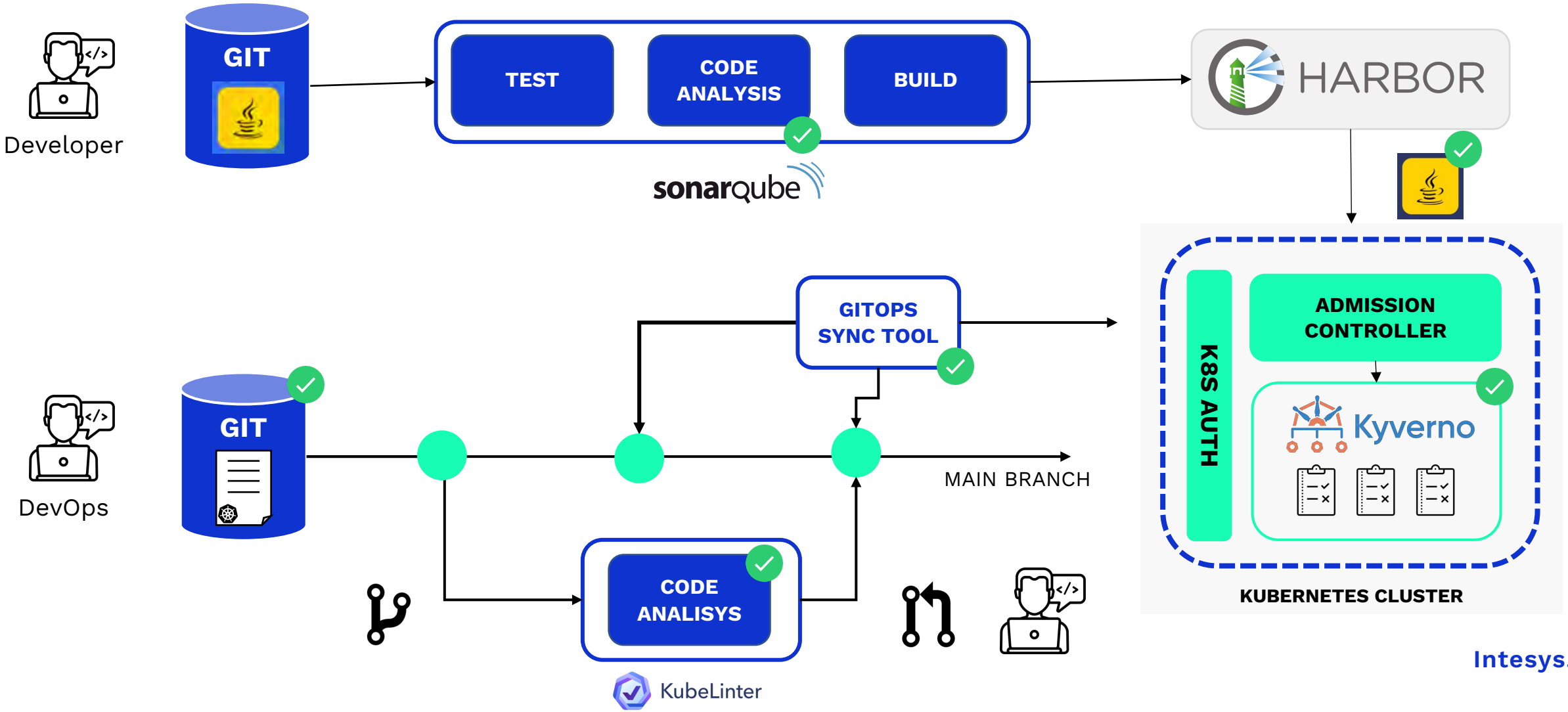
SESSIONE TECH

Kubernetes Secure GitOps Pipeline

Intesys.it


Developer
GIT
TEST
CODE ANALYSIS
BUILD
sonarqube
HARBOR
DevOps
GIT
CODE ANALYSIS
DEPLOY
KubeLinter
kubectl apply
AUTH
ADMISSION CONTROLLER
Kyverno
KUBERNETES CLUSTER


Developer
GIT
TEST
CODE ANALYSIS
BUILD
sonarqube
HARBOR
DevOps
GIT
Pull Changes
GITOPS SYNC TOOL
Sync Cluster
K8S AUTH
ADMISSION CONTROLLER
Kyverno
KUBERNETES CLUSTER


Developer
GIT
TEST
CODE ANALYSIS
BUILD
sonarqube
HARBOR
DevOps
GIT
GITOPS SYNC TOOL
MAIN BRANCH
CODE ANALISYS
KubeLinter
K8S AUTH
ADMISSION CONTROLLER
Kyverno
KUBERNETES CLUSTER

Headless & API date

SESSIONE TECH

GitOps in Kubernetes

Cosa ricordare?

- Utilizzo corretto del **repository manager Git**, del suo workflow approvativo e della sua gestione dei **ruoli e permessi**
- Scegliere un **tool di sync** (push o pull) che decide chi e su quali ambienti può installare applicazioni e configurazioni
- **Container Vulnerability Scanning** sui singoli container per salvaguardare la salute dell'intero cluster
- **Analisi Statica dei descrittori** inserita nella pipeline GitOps
- **Policy Manager** per validare le risorse che vengono inserite in Kubernetes

Headless & API date

Liferay | mia Platform | Intesys

Grazie

Enrico Costanzi

SOFTWARE DEVELOPER, INTESYS

enrico.costanzi@intesys.it