KubeCon | CloudNativeCon

North America 2023

Policy-based GRC

CNCF Kubernetes Policy WG

Hi, there!

Anca Sailer
Distinguished Engineer, IBM

Andy Suderman
CTO, Fairwinds

Jim Bugwadia
Founder & CEO, Nirmata

Poonam Lamba
Product Manager, Google

Robert Ficcaglia
CTO, SunStone Secure

Kubernetes Policy WG

Provide an overall architecture that describes both the current policy related implementations as well as future policy related proposals in Kubernetes. Through a collaborative method, we want to present both operators and users a universal view of policy architecture in Kubernetes.

Slack:
https://slack.k8s.io/#wg-policy

GitHub:
kubernetes-sigs/wg-policy-prototypes

Projects

- Kubernetes Policy Management Paper
- Policy Report CRD <API>
  - Policy Report Adapters: Trivy, Kyverno, kube-bench, Falco, …
  - Policy Report CRD → NIST OSCAL
- Kubernetes Governance, Risk, and Compliance Paper

Audience Question 1

For Kubernetes, how many are implementing or planning to implement:

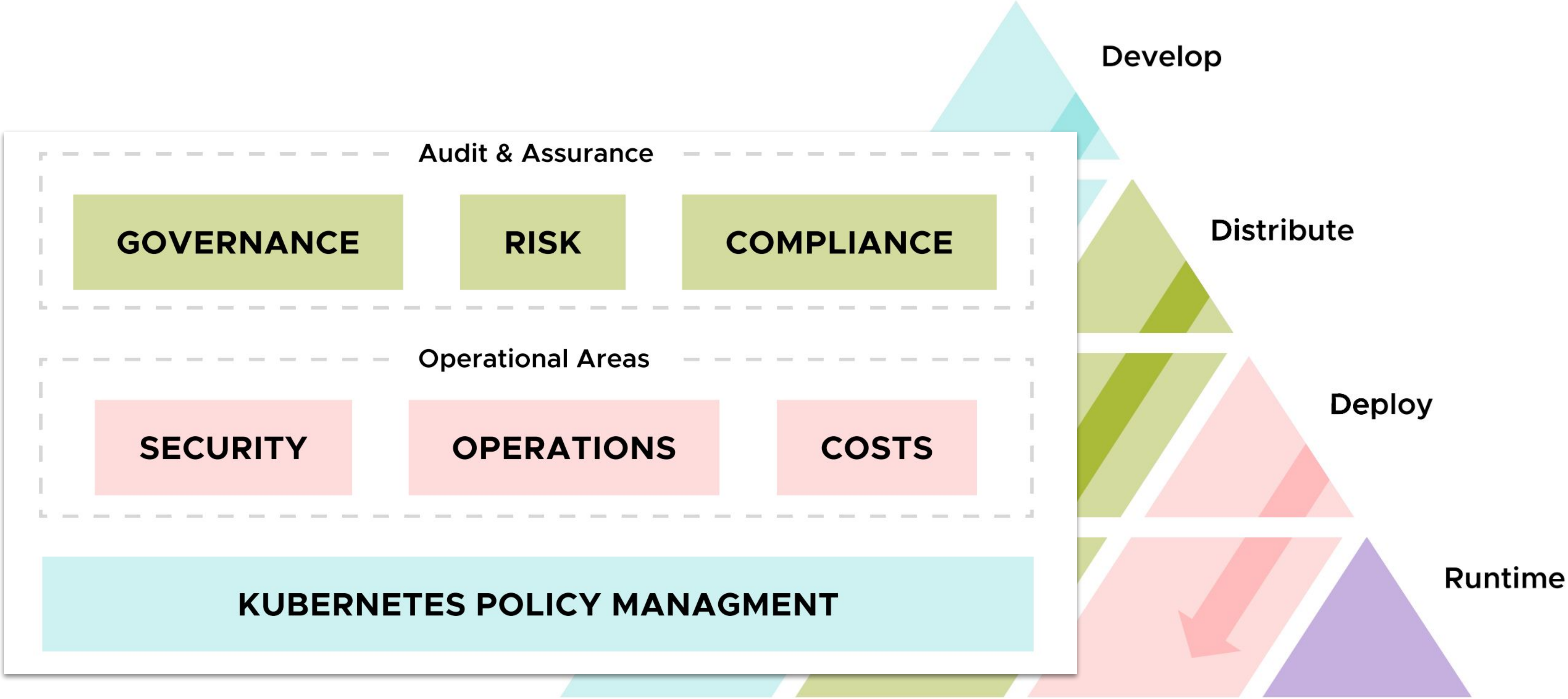
1. Any form of policies?
2. Policy as Code (via CI, GitOps, etc.)?
3. Compliance as Code?

Audience Question 2

What are your top pain points for Kubernetes policy & governance?

1. Deciding on a policy engine
2. Writing & managing policies
3. Mapping across policies, compliance standards and controls

Kubernetes GRC



Upcoming project ideas

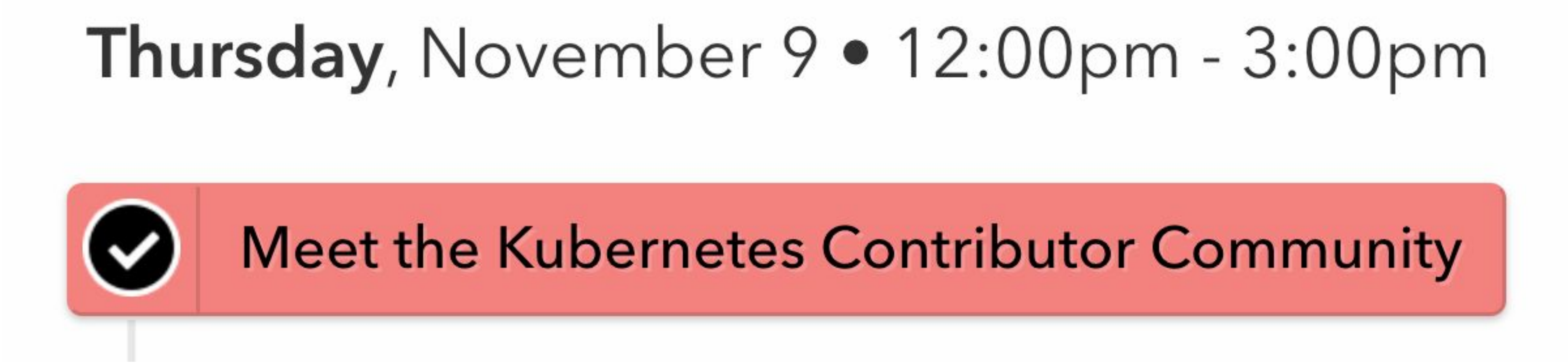
1. Map Kubernetes policies to compliance standards and controls?
2. Kubernetes controls catalog?

Meetings

Wed 8:00 AM Pacific, Every two weeks;

Join kubernetes-wg-policy@googlegroups.com to get a calendar invite

Let's continue the conversation…



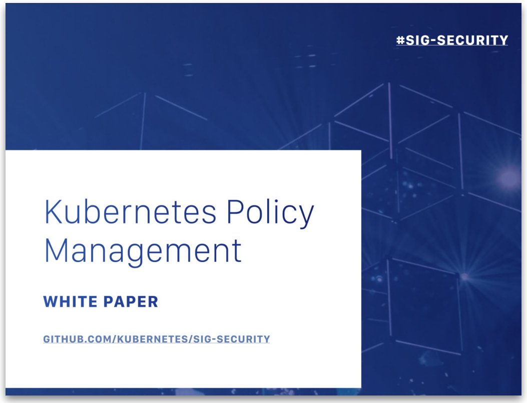
Thursday, November 9 • 12:00pm - 3:00pm

✓ Meet the Kubernetes Contributor Community

Please scan the QR Code above
to leave feedback on this session

Thanks!

Kubernetes Policy Management

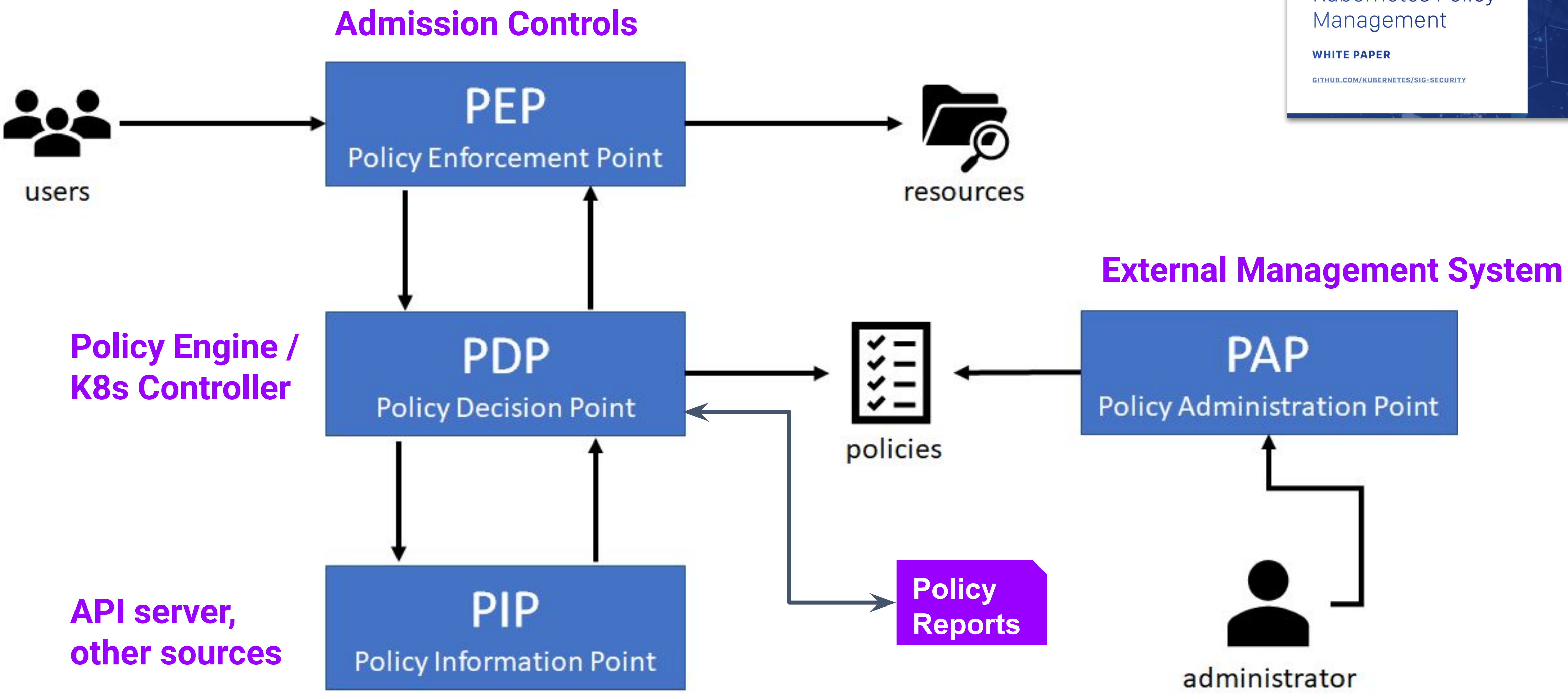


#SIG-SECURITY

Kubernetes Policy Management

WHITE PAPER

GITHUB.COM/KUBERNETES/SIG-SECURITY



Admission Controls

users

PEP

Policy Enforcement Point

resources

External Management System

Policy Engine / K8s Controller

PDP

Policy Decision Point

policies

PAP

Policy Administration Point

API server, other sources

PIP

Policy Information Point

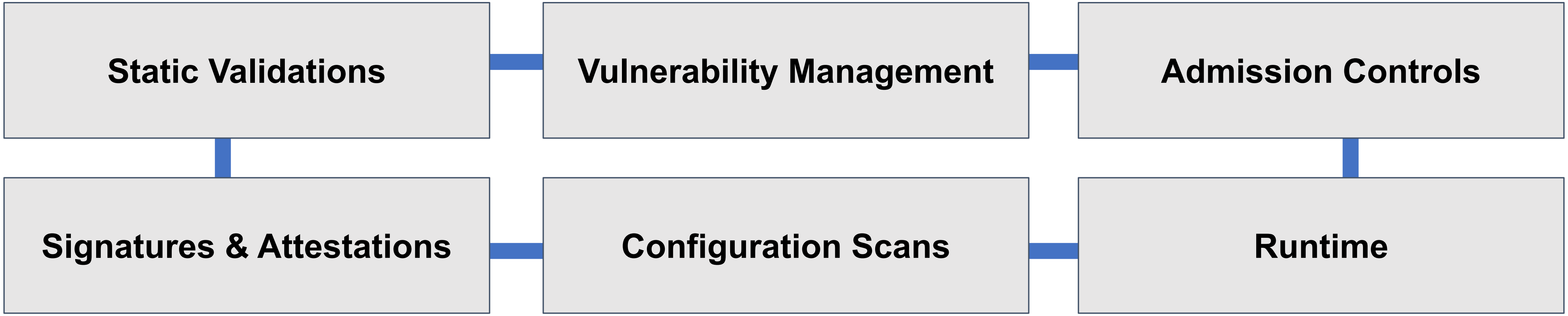
Policy Reports

administrator

https://github.com/kubernetes/sig-security/blob/main/sig-security-docs/papers/policy/CNCF_Kubernetes_Policy_Management_WhitePaper_v1.pdf

Kubernetes Policy Report CRD

Kubernetes Custom Resource Definition (CRD) in OpenAPI v3 schema that unifies reporting of Kubernetes security and compliance issues



Static Validations

Vulnerability Management

Admission Controls

Signatures & Attestations

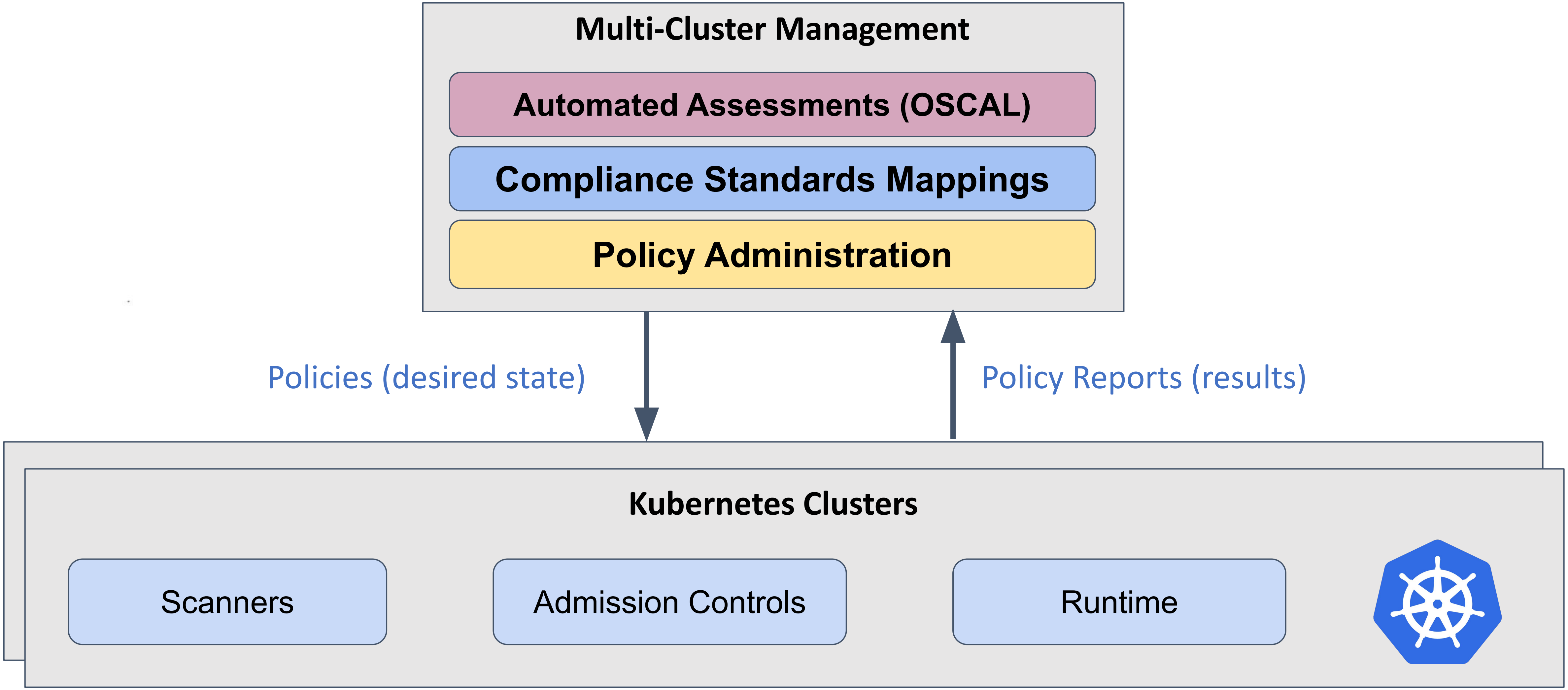
Configuration Scans

Runtime

Policy Report CRD

Tool	Area	Status
Kyverno	Configuration Security	Completed
kube-bench	CIS Kubernetes Benchmarks (Control plane, worker nodes)	Completed
Falco (Sidekick)	Runtime Security	Completed
Trivy	Vulnerability scanning	Completed
KubeArmor	Runtime Security	Completed
Policy Reporter	UI / Reporting / Notifications	Completed
OSCAL Policy Report	Trestle lib / cli	Completed

Policy - Compliance Mappings



Multi-Cluster Management

Automated Assessments (OSCAL)

Compliance Standards Mappings

Policy Administration

Policies (desired state)

Policy Reports (results)

Kubernetes Clusters

Scanners

Admission Controls

Runtime

IaC

CI/CD

Application Workloads

Question

What are the standards you want to be compliant with?

1. Pod Security Standards
2. NIST
3. CIS Kubernetes Benchmarks
4. CIS Standard Controls
5. PCI DSS