10/14/2023

Hacker-Proof Your Kubernetes Cluster with Kyverno Policies

PRESENTATION BY:

DIVYANSHU SHUKLA

Hello!

I am Divyanshu Shukla

6+ years of experience in bugbounty, pentesting, cloud security and secure coding review.

Acknowledged by Airbnb, Google, Microsoft, Apple, Samsung, Opera, AWS, Amazon, Mozilla.

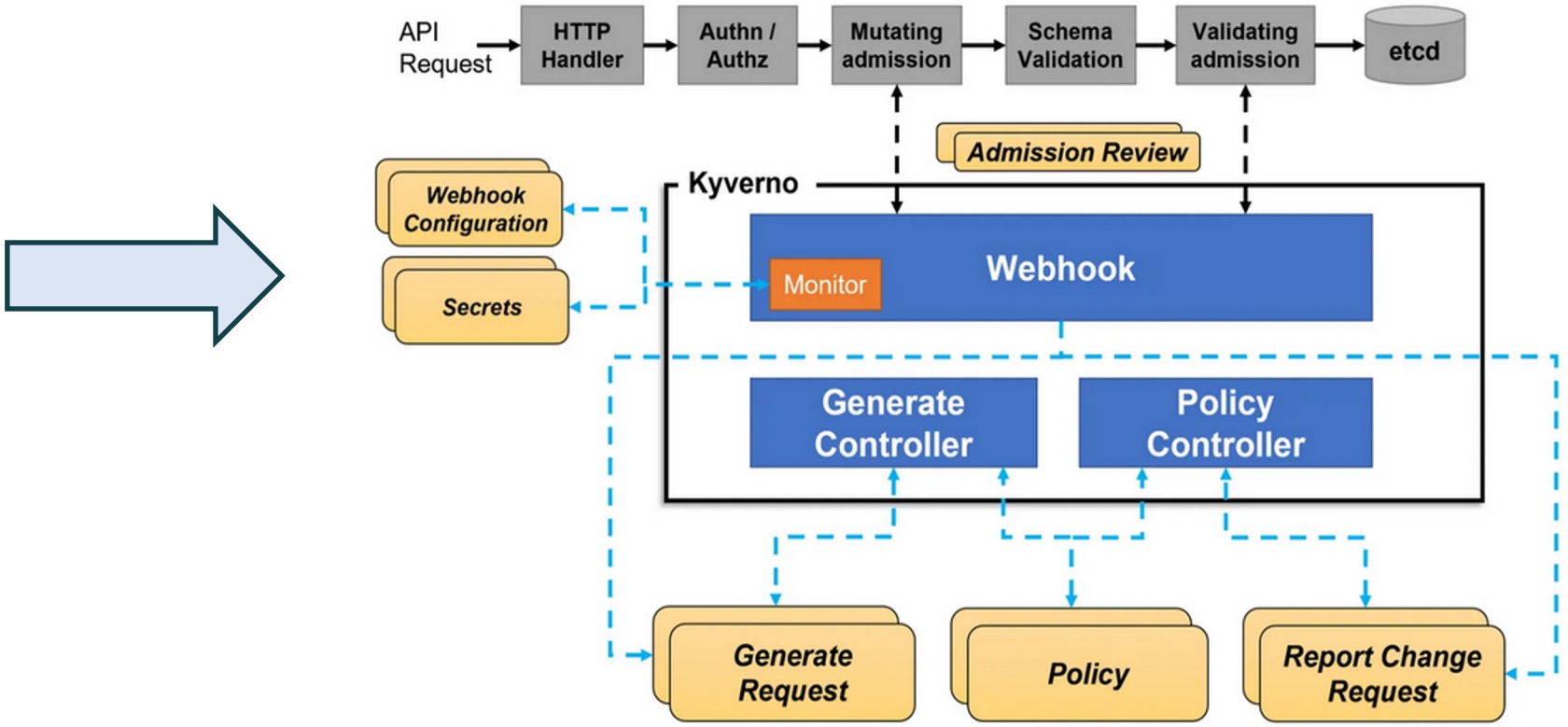
Trainer at Nullcon & Bsides, Crew Member at Defcon Cloudvillage & AWS Community Builder

AGENDA

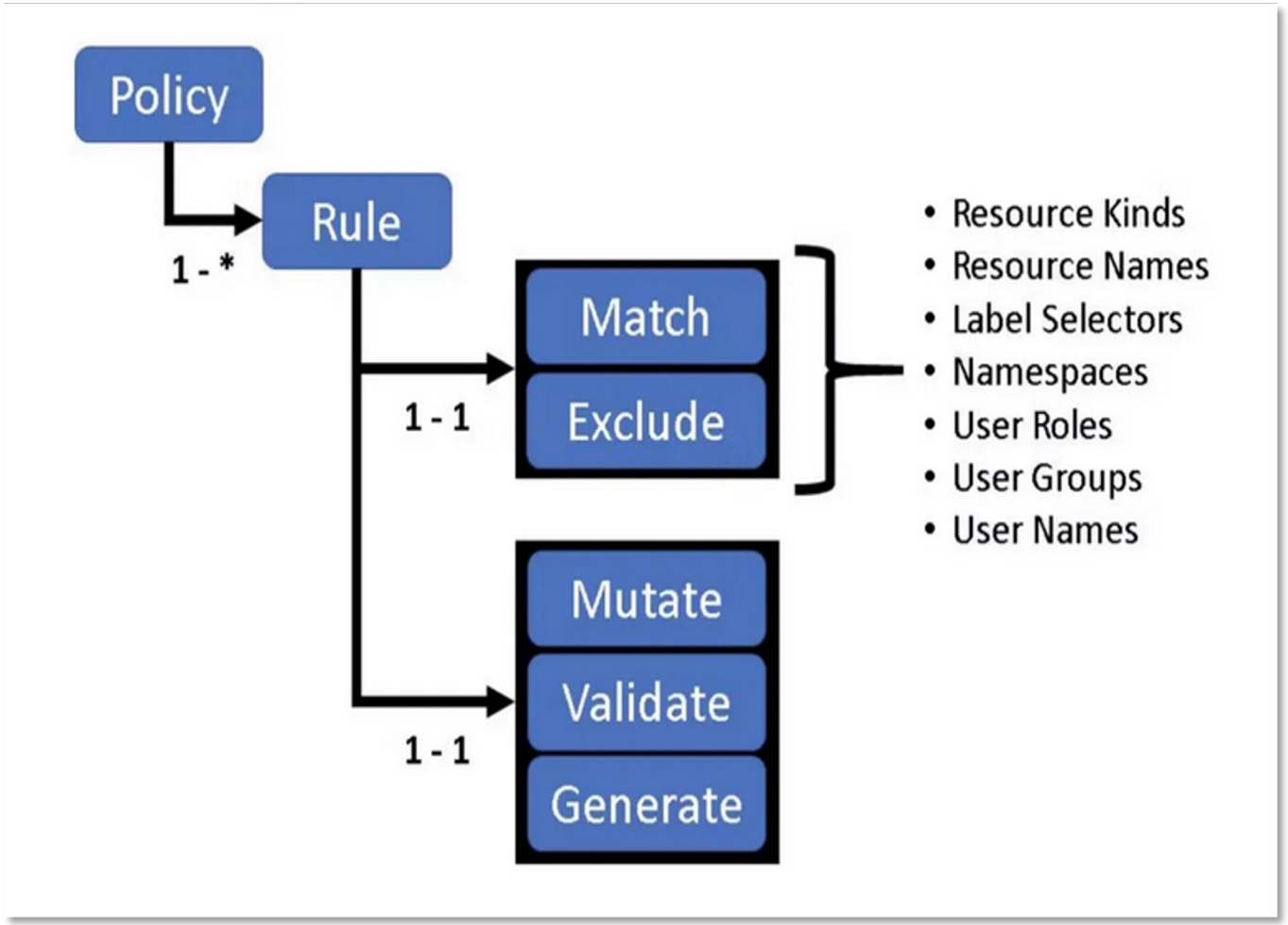
- Introduction
- How Kyverno Works ?
- Kyverno Policy Structure
- Demo
- Real-world Policy Examples

HOW KYVERNO WORKS ?

- Validation
- Mutation
- Generation



KYVERNO POLICY STRUCTURE



TOP POLICIES TO BLOCK ATTACKERS TO MAKE SECURE CLUSTER

REAL-WORLD POLICY EXAMPLES

- **Policy 1: blockpodexecnamespace.yaml**
  - Purpose: Ensuring restricted pod execution within specified namespaces.
- **Policy 2: disallowcreateapplypatchdelete.yaml**
  - Purpose: Restricting certain create, apply, patch, and delete operations.
- **Policy 3: disallowprivilegecontainer.yaml**
  - Purpose: Enforcing policies against privileged containers.

REAL-WORLD POLICY EXAMPLES

- **Policy 4: hostmountpath.yaml**
  - Purpose: Addressing security issues related to host-path mounts.

- **Policy 5: restrictbindingtoclusteradmin.yaml**
  - Purpose: Ensuring cluster-wide permissions are tightly regulated.

REAL-WORLD POLICY EXAMPLES

- **Policies 6: restrictnodeselectionworker1.yaml & restrictnodeselectionworker2.yaml**
  - Purpose: Managing node affinity and taints for workload scheduling.

- **Policy 7: runasnonroot.yaml**
  - Purpose: Promoting the best practice of running containers as non-root users.

ANY QUESTIONS ??

THANK YOU!

You can find me at

/@justm0rph3u5