

Runtime security for vCluster using Falco

@saiyampathak

Hi I'm Saiyam



Saiyam Pathak (@saiyampathak)

Principal Developer Advocate at Loft Labs

- Founder @Kubesimplify, @BuildSafe
- Previously at Civo, Walmart, Oracle, and HP
- Written books on CKA and CKS
- Kubestronaut

@saiyampathak





Companies create a lot of Kubernetes clusters



- Cluster per team
- Cluster per environment
- Duplication of resources

COST?
Maintenance?

SO MANY CLUSTERS !!

= 1000s of clusters

Companies create a lot of Kubernetes clusters



Control plane costs



Platform stack costs

Cloud spend is on the rise.

Gartner forecasts worldwide public cloud spending to reach **\$679 billion** in 2024, 20.4% increase from 2023

**70% of organizations identified
overprovisioned Kubernetes
as the leading cause for
their surge in spend**



CLOUD NATIVE
COMPUTING FOUNDATION

2023 Cloud Native & K8s
Finops Microsurvey


```
graph LR; A[Multi Tenancy] --> B[Strong Isolation]; A --> C[Cost Savings]; A --> D[Less complexity]
```

Multi Tenancy

Strong Isolation

Cost Savings

Less complexity

How to do multi Tanency?



```
graph TD; A[How to do multi Tanency?] --> B[Workload Isolation]; A --> C[Fair Use of Resources]; A --> D[Tenant Autonomy];
```

Workload Isolation

Fair Use of Resources

Tenant Autonomy

Workload Isolation?

```
apiVersion: v1
kind: Namespace
metadata:
  name: tenant-1
  labels:
    pod-security.kubernetes.io/enforce: restricted
    pod-security.kubernetes.io/audit: restricted
    pod-security.kubernetes.io/warn: restricted
```

Networking Isolation?

Deny everything internal

= Allow everything but except
internal IPs

Allow tenant namespace(s)

Allow DNS servers (all?)

Allow Kubernetes API

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: default-policy
  namespace: tenant-1
spec:
  policyTypes:
    - Egress
  egress:
    - to:
        - ipBlock:
            cidr: 0.0.0.0/0
            except:
              - 100.64.0.0/10
              - 127.0.0.0/8
              - 10.0.0.0/8
              - 172.16.0.0/12
              - 192.168.0.0/16
        - namespaceSelector:
            matchLabels:
              tenant: tenant-1
    - ports:
        - port: 53
          protocol: UDP
        - port: 53
          protocol: TCP
    - ports:
        - port: 443
        - port: 8443
      to:
        - ipBlock:
            cidr: ${KUBE_API}/32
```


Fair resource usage

Number of objects

Custom Resources: `count/<resource>.<group>`

Node Ports

Load Balancers

Hardware Resources

```
apiVersion: v1
kind: ResourceQuota
metadata:
  name: default-quota
  namespace: tenant-1
spec:
  hard:
    count/pods: 20
    count/secrets: 100
    count/configmaps: 100
    count/persistentvolumeclaims: 20
    count/services: 20
    count/endpoints: 40
    count/virtualservice.networking.istio.io: 10
    services.nodeports: 0
    services.loadbalancers: 0
    requests.cpu: 10
    requests.memory: 20Gi
    requests.storage: 100Gi
    requests.ephemeral-storage: 60Gi
    limits.cpu: 20
    limits.memory: 40Gi
    limits.ephemeral-storage: 160Gi
```

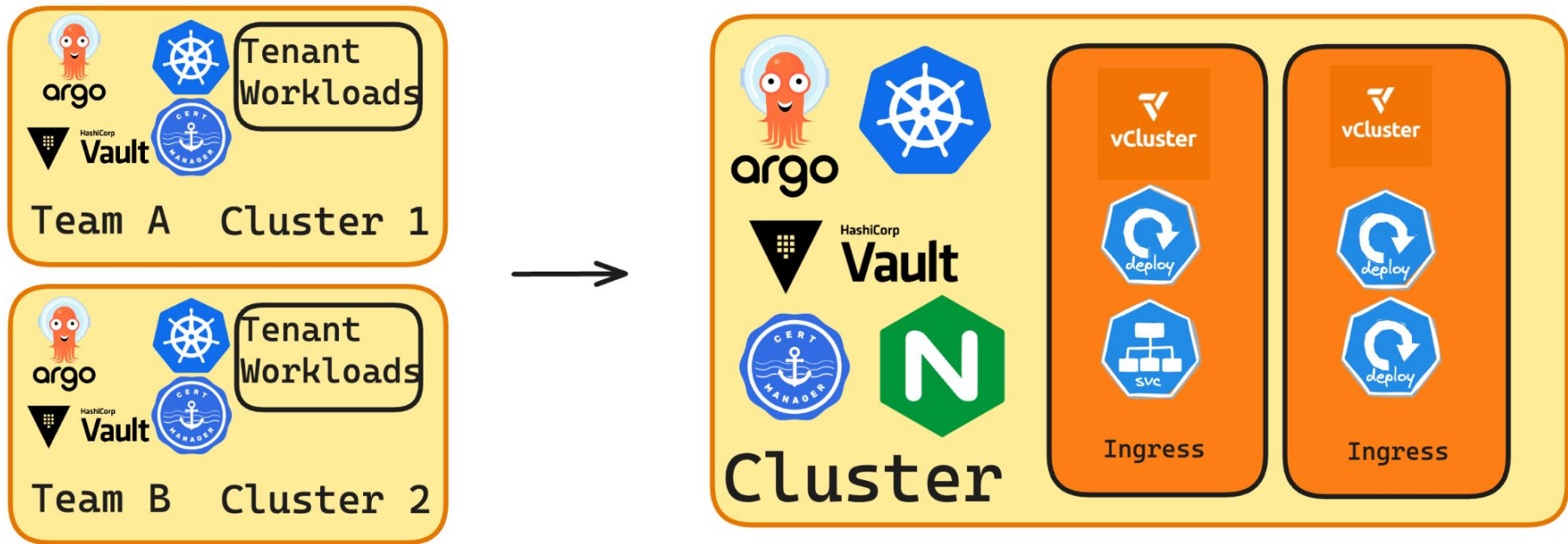
Namespace per tenant?

- ❏ *Sharing Normal Clusters between teams*
- ❏ *Segregate by Namespace*
 - *Prevents naming conflicts*
 - *Many isolation controls are namespace-based*
 - *Many tools provide easy namespace-based filtering*
- ❏ *Namespace = Tenant's Realm*

Namespace: Are they enough?

- ❑ *Security Consideration with PVC*
- ❑ *Hard to configure some isolation controls*
- ❑ *1 Config → Config per tenant*
- ❑ *Complexity grows with number of tenants*
- Cluster Wide Resources*
- ❑ *Custom Resource Definitions (CRDs)*
- ❑ *Controllers*

Multi-tenancy with virtual clusters



Multi-tenancy with virtual clusters



Control Plane Per Tenant

- Full cluster admin access for tenant
- Reduced complexity in host cluster
- Super lightweight, fast, and cheap




Deploy via CLI, Helm, Argo, TF, ...



Isolation Best Practices Built-In

```
# vcluster.yaml
policies:
  networkPolicy:
    enabled: true
  resourceQuota:
    enabled: true
  limitRange:
    enabled: true
```

Type of Sharing: virtual clusters

	Separate Namespace For Each Tenant	 vcluster	Separate Cluster For Each Tenant
Isolation	very weak	strong	very strong
Access For Tenants	very restricted	vcluster admin	cluster admin
Cost	very cheap	cheap	expensive
Resource Sharing	easy	easy	very hard
Overhead	very low	very low	very high

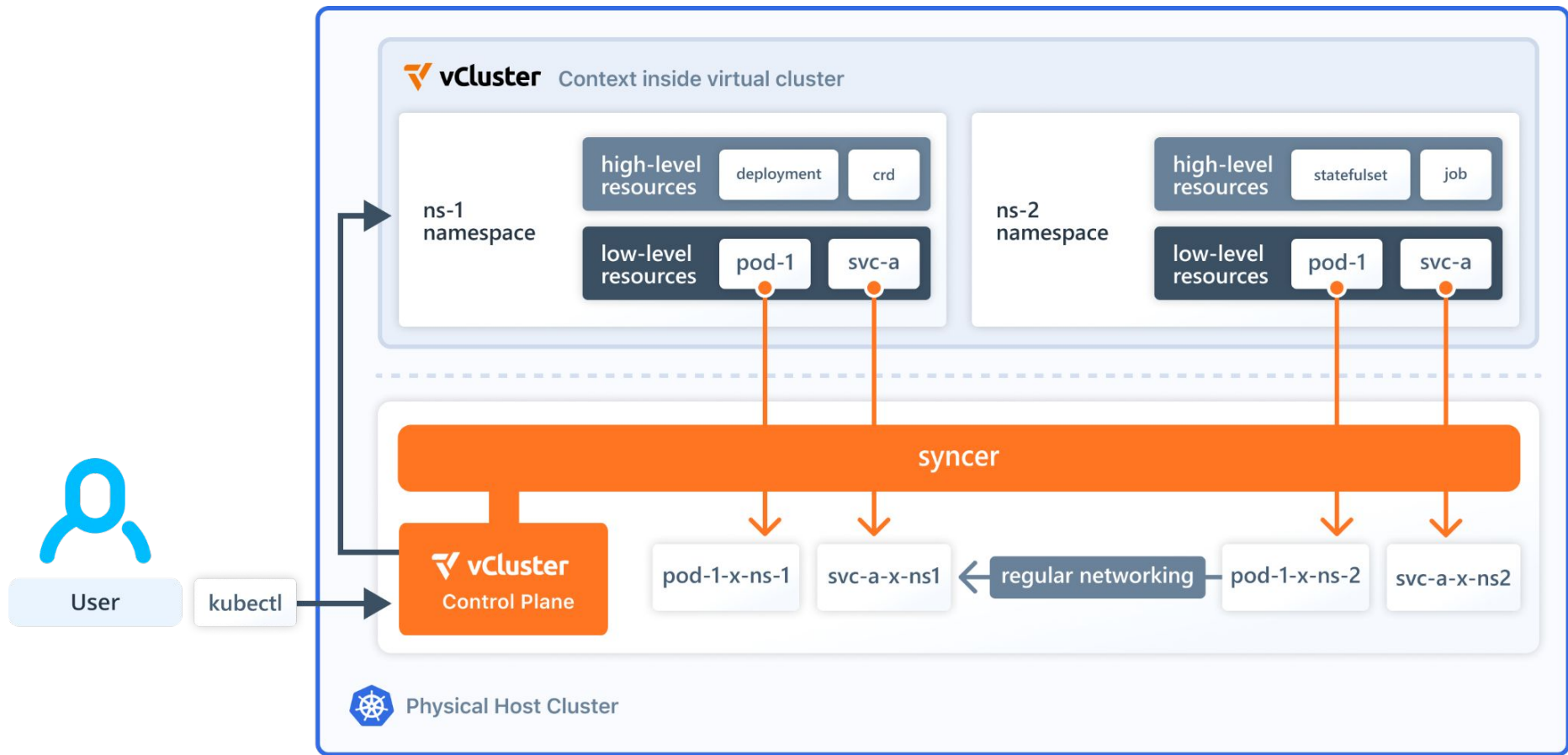
Virtual Clusters: What they bring in?

- ❏ *Idle & Underutilized Clusters*
- ❏ On-Hold / Forgotten Clusters
- ❏ Autonomy & Responsibility Challenges

VClusters: What are they?

- ❑ *KUBERNETES IN KUBERNETES*
- ❑ *Can deploy fast as containers*
- ❑ *Can save control plane costs*
- ❑ *Isolation Sync resources*
- ❑ *Self service capabilities*
- ❑ *Improved DX*

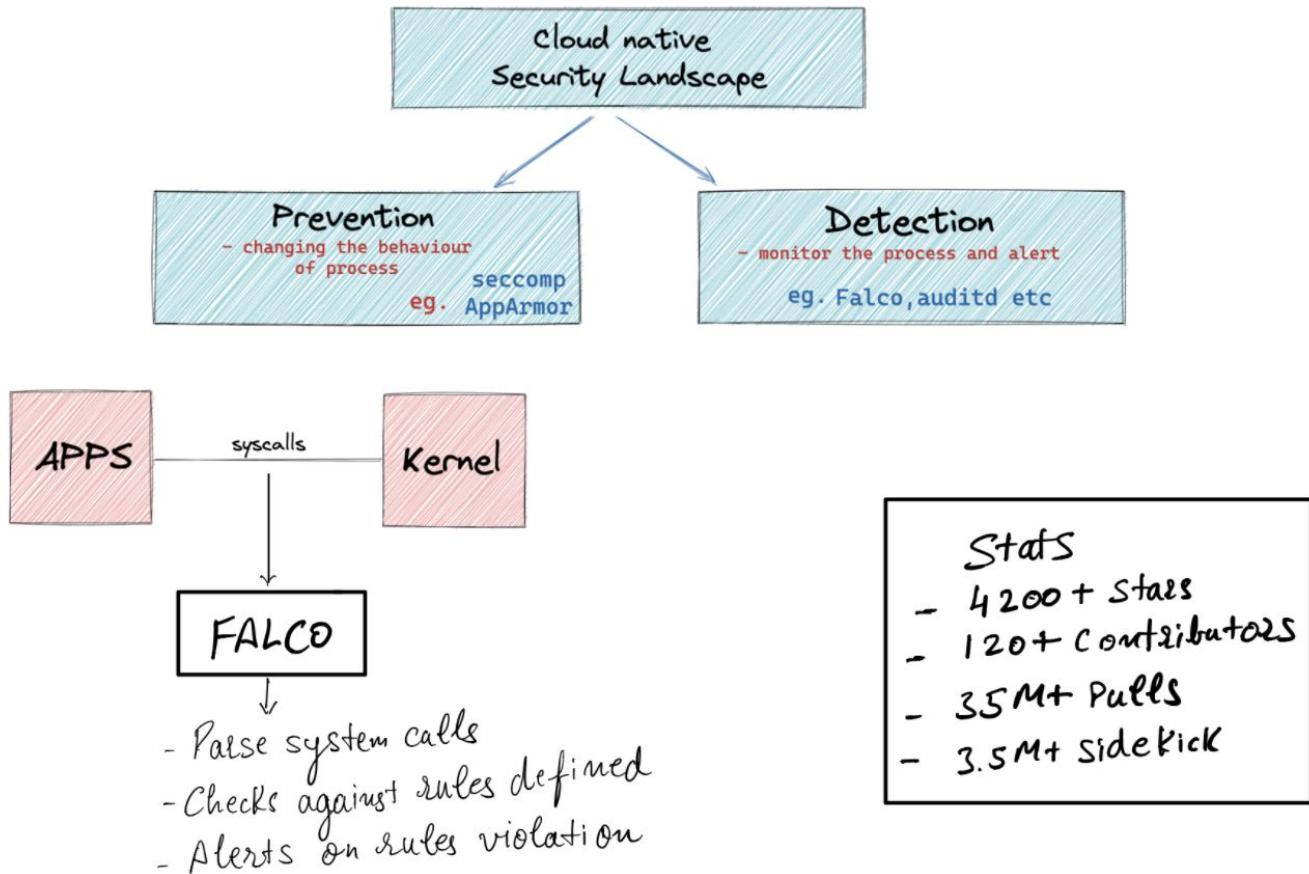


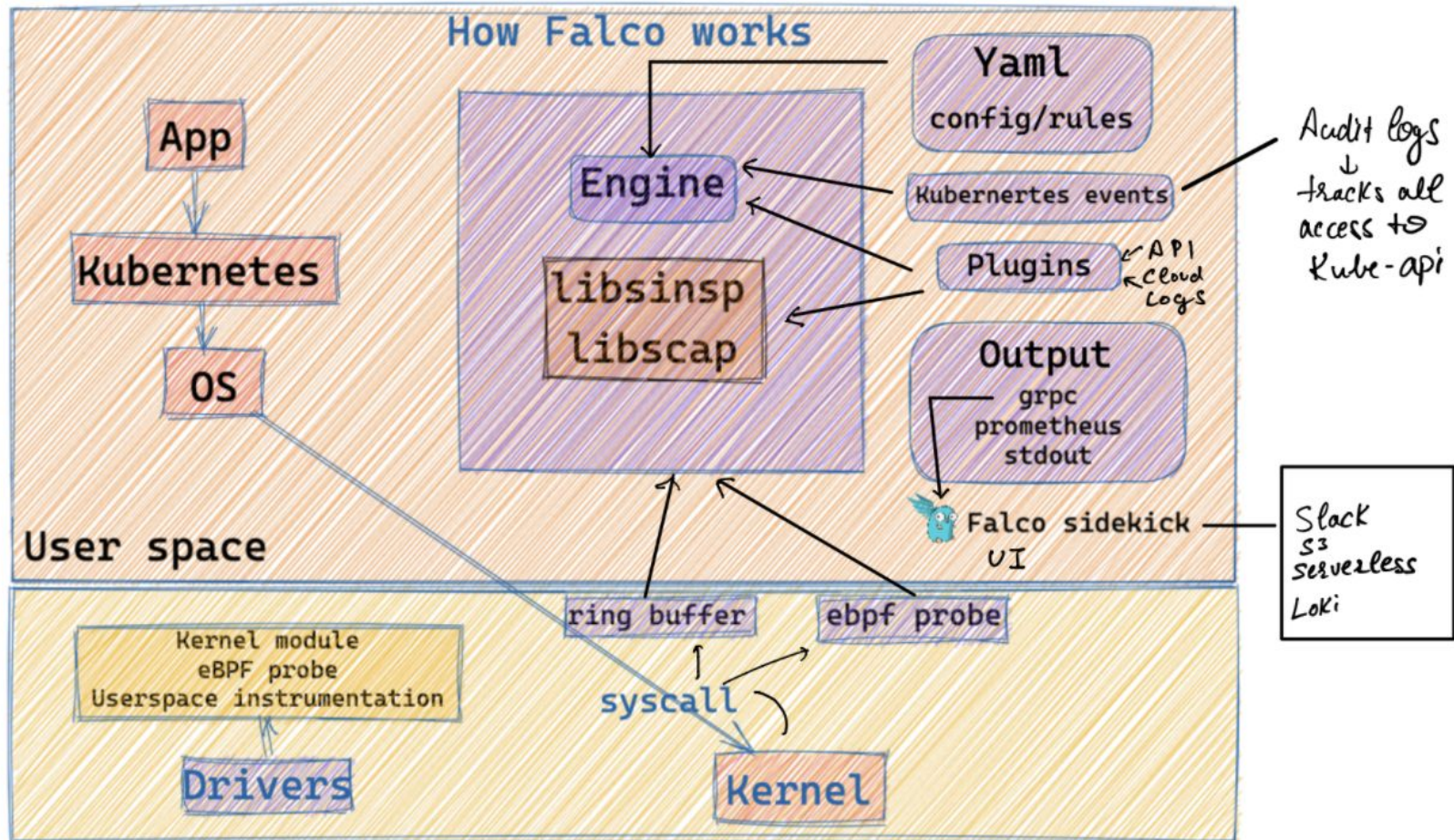


Falco

Introduction

Falco, the cloud-native runtime security project,
is the de facto Kubernetes threat detection engine

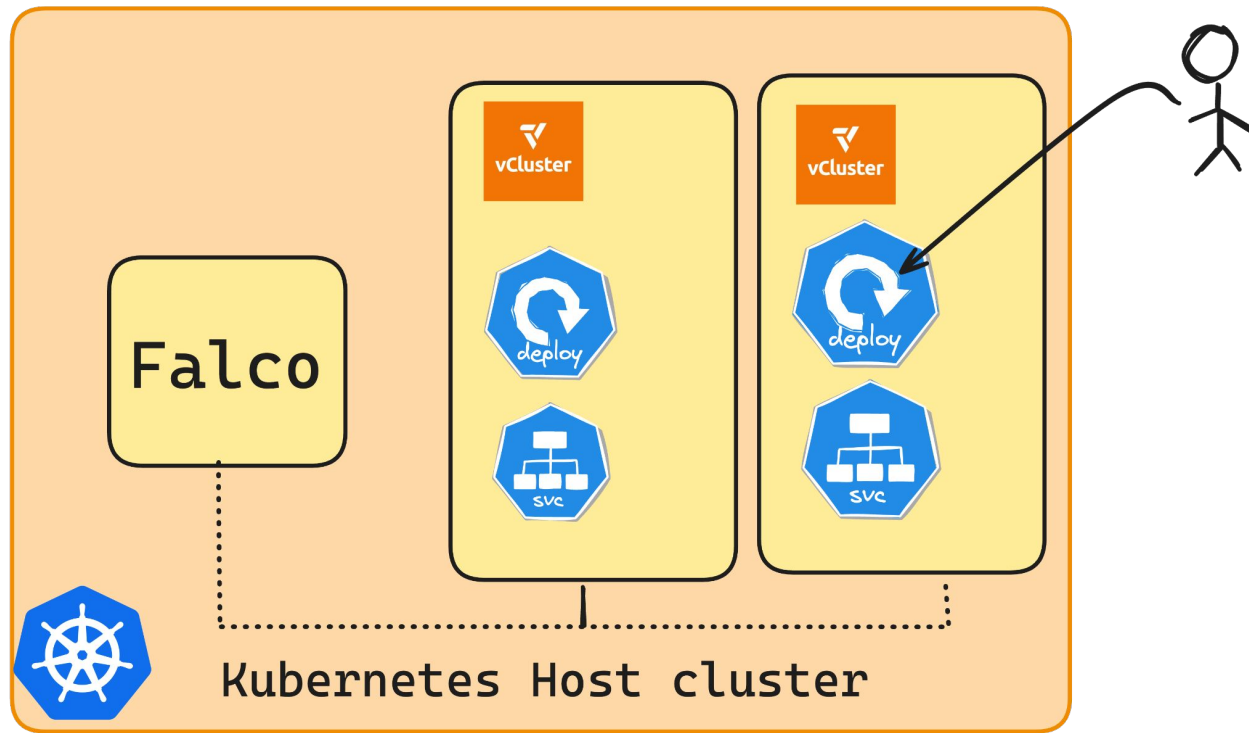





```
15:35:48.045077665: Warning Sensitive file opened for reading by non-trusted program (file=/etc/shadow gparent=systemd ggp  
parent=<NA> gggparent=<NA> evt_type=open user=root user_uid=0 user_loginuid=-1 process=cat proc_exepath=/bin/cat parent=container  
d-shim command=cat /etc/shadow terminal=34816 container_id=1f6a01b8f69f container_image=docker.io/securecodebox/dummy-ssh con  
tainer_image_tag=v1.0.0 container_name=dummy-ssh k8s_ns=vcluster k8s_pod_name=my-dummy-ssh-864c9db6f4-fnjpk-x-default-x-ssh)  
15:37:18.251611761: Warning Sensitive file opened for reading by non-trusted program (file=/etc/shadow gparent=sshd ggp  
parent=sshd gggparent=containerd-shim evt_type=open user=root user_uid=0 user_loginuid=0 process=cat proc_exepath=/bin/cat parent=ba  
sh command=cat /etc/shadow terminal=34816 container_id=1f6a01b8f69f container_image=docker.io/securecodebox/dummy-ssh contain  
er_image_tag=v1.0.0 container_name=dummy-ssh k8s_ns=vcluster k8s_pod_name=my-dummy-ssh-864c9db6f4-fnjpk-x-default-x-ssh)  
^C
```

<https://gist.github.com/saiyam1814/603b47666f68c530ac2809a98b66b6cc>

Falco and vCluster



Q&A and ME:



saiyampathak



saiyam1814



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

