

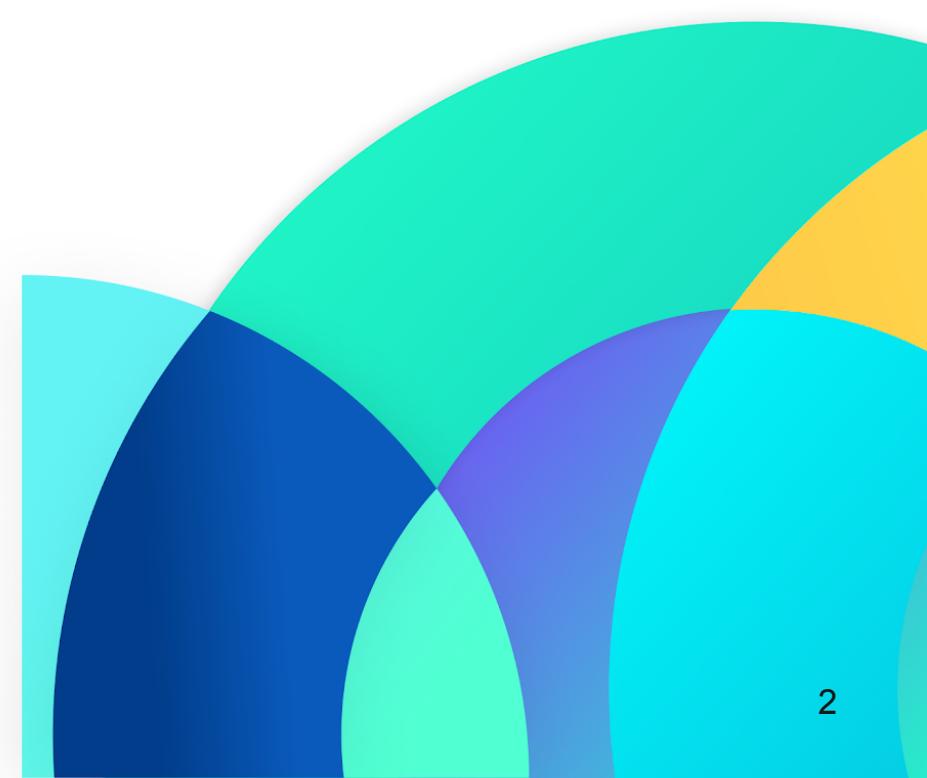
# OWASP Kubernetes



Miguel Hernández  
**Staff Threat Research Engineer**  
**Sysdig**

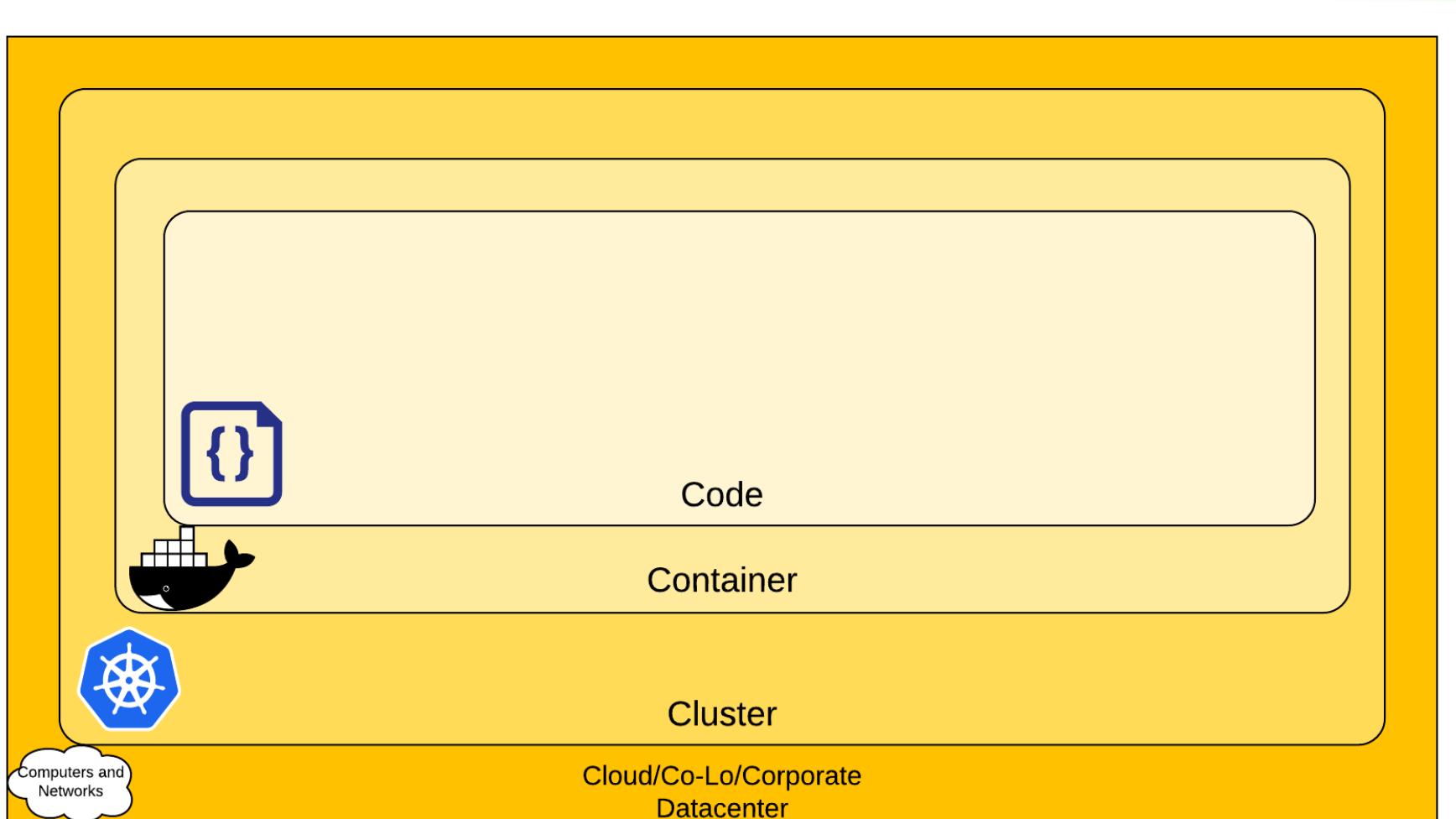
# Agenda

1. What is the OWASP Kubernetes Top 10?
2. Why are Kubernetes risks so concerning?
3. What are the common security risks?
  - What's needed to address the risks?



**1. What is the OWASP  
Kubernetes Top 10?**

# The 4C's of Cloud Native security



<https://kubernetes.io/docs/concepts/security/overview/>

# Kubernetes CIS Benchmark



**Center for  
Internet Security®**

*Creating Confidence in the Connected World.™*

## Recent versions available for CIS Benchmark:

- Alibaba Cloud Container Service For Kubernetes (ACK)  
(1.0.0)
- Amazon Elastic Kubernetes Service (EKS) (1.3.0)
- Azure Kubernetes Service (AKS) (1.3.0)
- Google Kubernetes Engine (GKE) (1.4.0)
- Kubernetes (1.7.1)
- Kubernetes V1.24 (1.0.0)
- Kubernetes V1.23 (1.0.1)
- Kubernetes V1.20 (1.0.1)
- Oracle Cloud Infrastructure Container Engine for  
Kubernetes(OKE) (1.3.0)
- RedHat OpenShift Container Platform (1.4.0)
- RedHat OpenShift Container Platform v4 (1.1.0)

<https://www.cisecurity.org/benchmark/kubernetes>

# MITRE ATT&CK Containers Matrix

ATT&CK®

Matrices ▾ Tactics ▾ Techniques ▾ Data Sources Mitigations ▾ Groups Software Campaigns

ATT&CKcon 4.0 will be held on Oct 24-25 in McLean, VA. [Click here](#) for more details and to register.

Home > Matrices > Containers

## Containers Matrix

View on the ATT&CK® Version Permalink

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise covering techniques against container technologies. The Matrix contains information for the Containers platform.

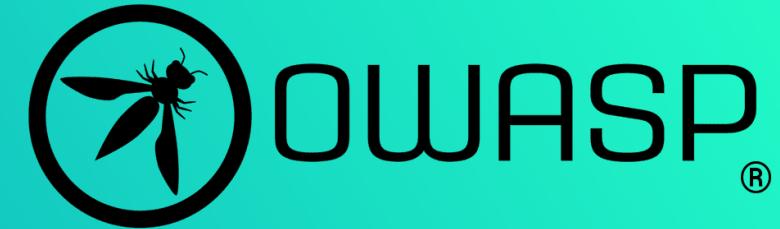
layout: side ▾ show sub-techniques hide sub-techniques help

Initial Access 3 techniques	Execution 4 techniques	Persistence 4 techniques	Privilege Escalation 4 techniques	Defense Evasion 7 techniques	Credential Access 3 techniques	Discovery 3 techniques	Lateral Moveme 1 techniques
Exploit Public-Facing Application	Container Administration Command	External Remote Services	Escape to Host	Build Image on Host	Brute Force (3)	Container and Resource Discovery	Use Alternate Authentication Material (1)
External Remote Services	Deploy Container	Implant Internal Image	Exploitation for Privilege Escalation	Deploy Container	Steal Application Access Token	Network Service Discovery	
Valid Accounts (2) □	Scheduled Task/Job (1) □	Scheduled Task/Job (1) □	Scheduled Task/Job (1) □	Impair Defenses (1) □	Unsecured Credentials (2) □	Permission Groups Discovery	
	User Execution (1) □	Valid Accounts (2) □	Valid Accounts (2) □	Indicator Removal	Masquerading (1) □		
				Valid Accounts (2) □	Use Alternate Authentication Material (1) □		
					Valid Accounts (2) □		

<https://attack.mitre.org/matrices/enterprise/containers/>

## What is Open Web Application Security Project (OWASP)?

- Open-source community
- Create awareness aids like the Top 10
- Develop and maintain OSS tools
- The first Top 10 is broader application security
- Kubernetes T10 was launched in 2022  
<https://owasp.org/www-project-kubernetes-top-ten/>



PROJECTS CHAPTERS

### OWASP Kubernetes Top Ten

Main

#### About the Kubernetes Top 10

When adopting [Kubernetes](#), we introduce new risks to our applications. This page provides an overview of these risks, aimed at helping security practitioners, system administrators, and Kubernetes users understand the Kubernetes ecosystem. The Top Ten is a prioritized list of these risks. In the future, we will expand this list to include other Kubernetes components and organizations varying in maturity and complexity.

#### Top 10 Kubernetes Risks - 2022

- K00: Welcome to the Kubernetes Security Top Ten
- K01: Insecure Workload Configurations
- K02: Supply Chain Vulnerabilities
- K03: Overly Permissive RBAC Configurations
- K04: Lack of Centralized Policy Enforcement
- K05: Inadequate Logging and Monitoring
- K06: Broken Authentication Mechanisms
- K07: Missing Network Segmentation Controls
- K08: Secrets Management Failures
- K09: Misconfigured Cluster Components
- K10: Outdated and Vulnerable Kubernetes Components
- Other Risks to Consider

# OWASP Kubernetes Top 10



K01 - Insecure Workload Configurations

K02 - Supply Chain Vulnerabilities

K03 - Overly Permissive RBAC

K04 - Policy Enforcement

K05 - Inadequate Logging

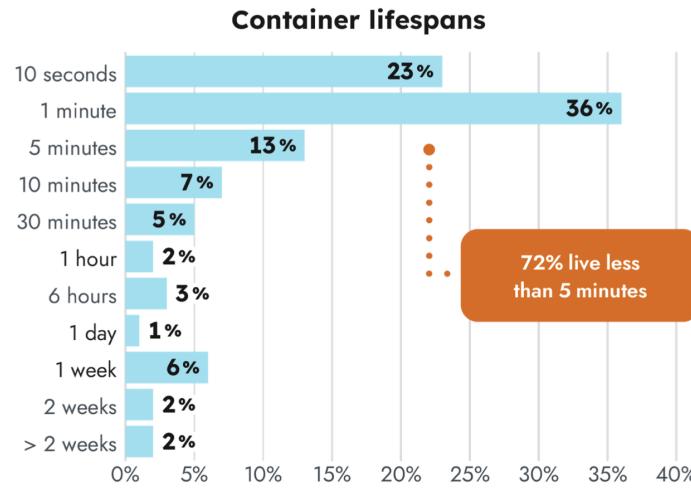
K06 - Broken Authentication

K07 - Network Segmentation

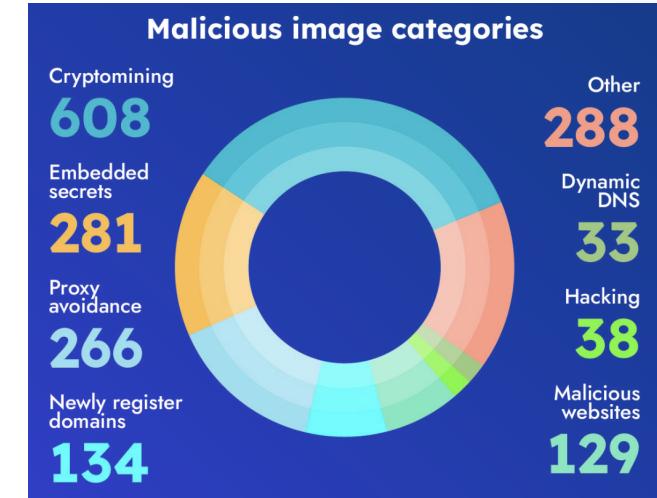
K08 - Secret Management

## 2. Why are Kubernetes risks so concerning?

# The security risks are real



Containers are ephemeral by nature



Dependencies have latent problems



Organizations struggle to keep pace with vulnerabilities



Security hygiene is lacking

# Expectation



# Reality



**3. What are the common security risks?**

# OWASP Kubernetes Top 10

## Misconfigurations

K01 - Insecure Workload Configurations

K09 - Misconfigured Cluster Components

K03 - Overly Permissive RBAC

K07 - Network Segmentation

## Lack of visibility

K05 - Inadequate Logging

K04 - Policy Enforcement

K08 - Secret Management

## Vulnerability management

K02 - Supply Chain Vulnerabilities

K06 - Broken Authentication

K10 - Vulnerable K8s Components

# K01 - Insecure Workload Configurations



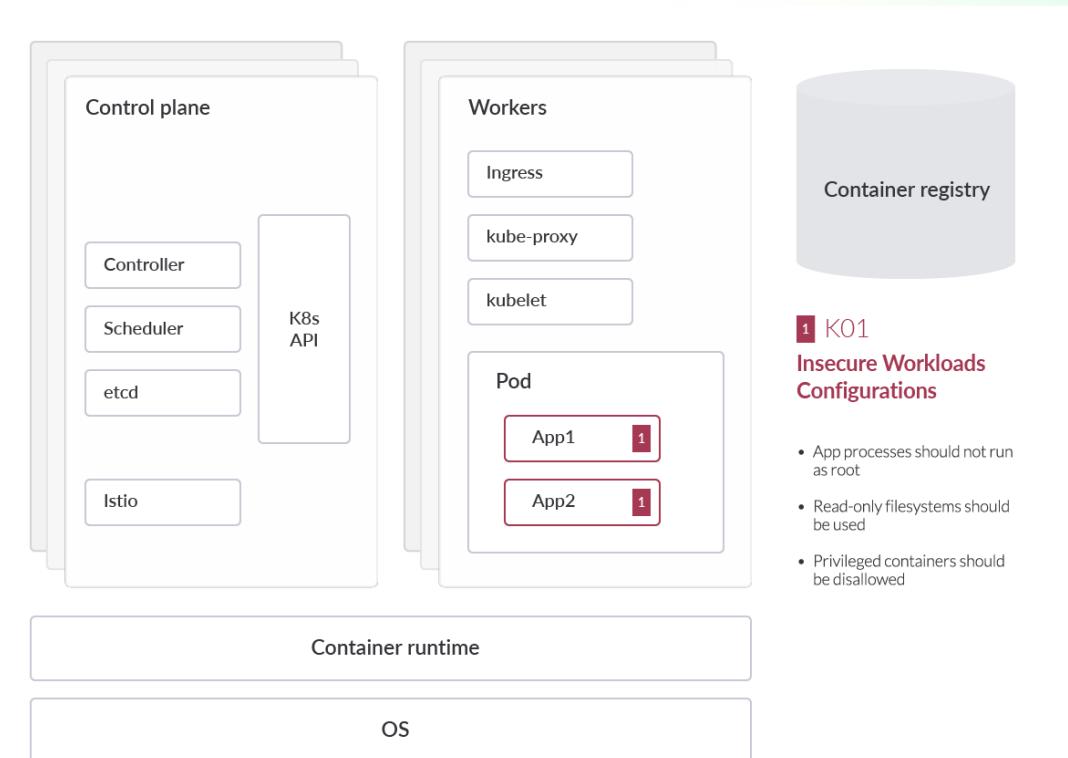
Run minimal, streamlined images in your containerized workloads, such as **Alpine Linux** images



Avoid defining deployments with '**privileged=true**' for your workloads



Configuring **readOnlyRootFilesystem: true** reduces the attack surface dramatically



# DEMO TIME

- Breaking out of a container inside a misconfigured Pod in kubernetes.
  - [https://www.youtube.com/watch?v=ZbHVRoWEwA8&ab\\_channel=Sysdig](https://www.youtube.com/watch?v=ZbHVRoWEwA8&ab_channel=Sysdig)

```
634bd4b5d3f6  docker:latest  docker-entrypoint.s...  5 minutes ago  Up 5 minutes          DooD
root@634bd4b5d3f6:/ # docker run -d -v /:/host --name escape --privileged --cap-add=ALL --pid=host --userns=host
ubuntu sleep 3600
1696c1fd64820bfd0ce197a8bf2e3ca994cd3d44835bd0f073266d3850ab9875
root@634bd4b5d3f6:/ # docker ps
CONTAINER ID        IMAGE               COMMAND             CREATED            STATUS              PORTS          NAMES
1696c1fd6482        ubuntu              "sleep 3600"        3 seconds ago     Up 2 seconds           escap...
e
656abfe3c4e7        ubuntu              "sleep 3600"        About a minute ago   Up About a minute      lucid...
_gagarin
634bd4b5d3f6        docker:latest       "docker-entrypoint.s..."  6 minutes ago     Up 6 minutes          DooD
root@634bd4b5d3f6:/ # docker exec -it escape bash
root@1696c1fd6482:/# █
```

# K02 - Supply Chain Vulnerabilities



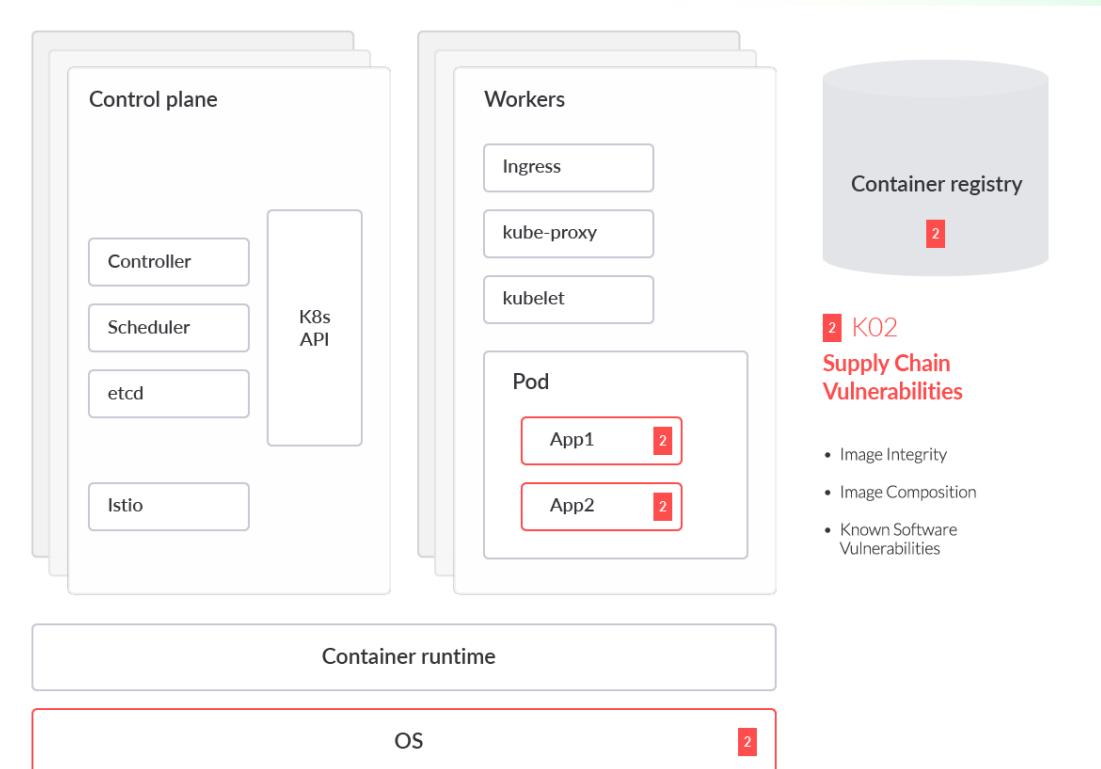
A **container image** represents binary data that encapsulates an application and all of its software dependencies.

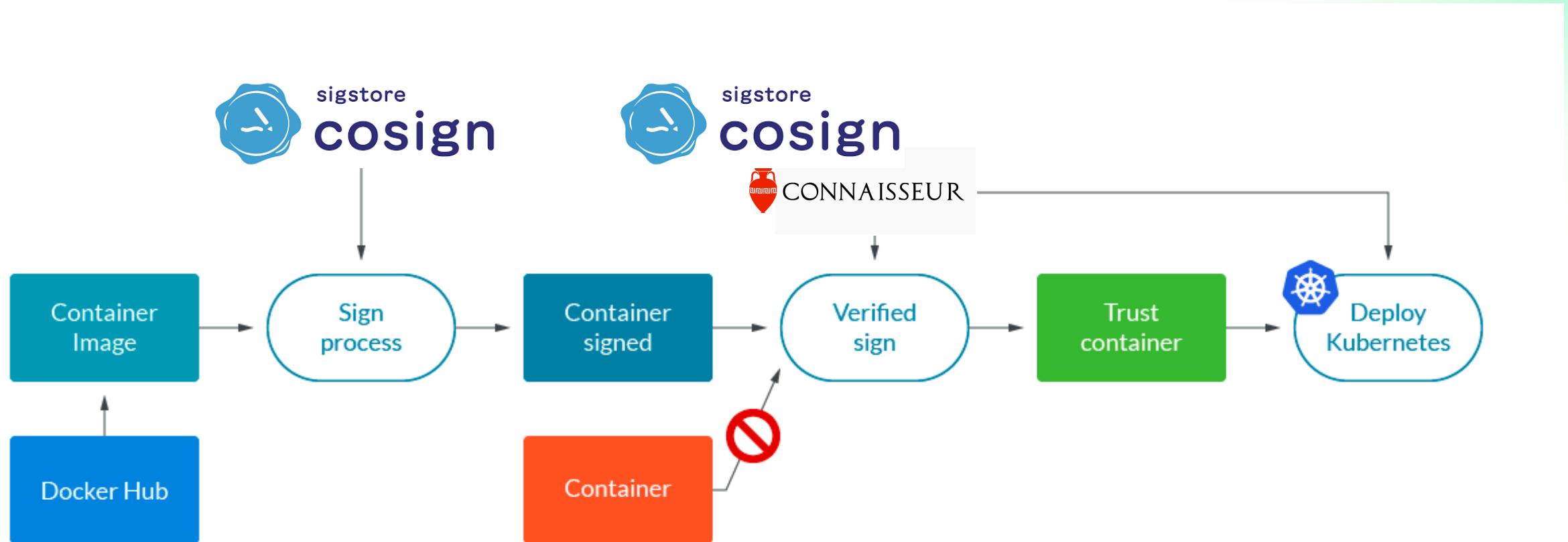


Even “small” clusters can have way more **service dependencies** than anticipated by virtue of containers and orchestration.



Another layer of security we can add is a process of **signing and verifying the images** we send to our registries or repositories.





# K03 - Overly-Permissive RBAC



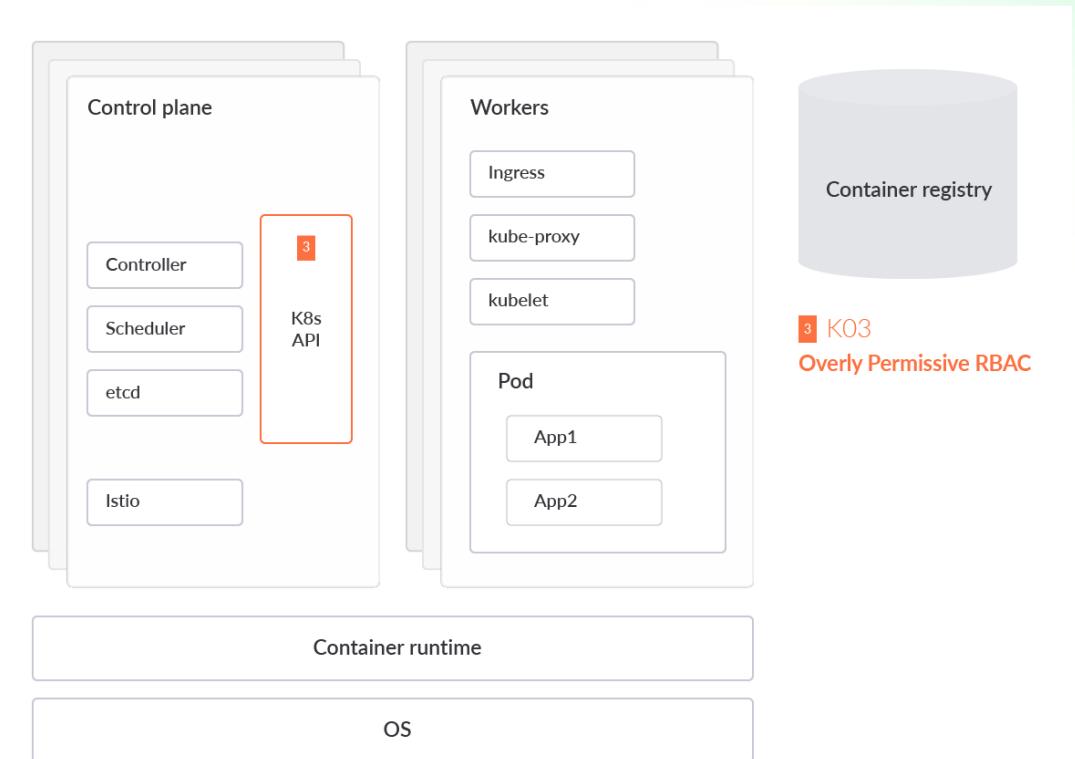
**RBAC Audit** is a tool designed to scan the Kubernetes cluster for risky roles within RBAC and requires python3



**Kubiscan** is a tool designed for scanning K8s clusters for risky permissions in the K8s' RBAC authorization model – not the RBAC roles.



**Krane** provides a dashboard of the cluster's current RBAC security posture and lets you navigate through its definition.



# RBAC

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole

metadata:
  name: aggregatedClusterRole1

aggregationRule:
  clusterRoleSelectors:
  - matchLabels:
    label1: value1

# The control plane automatically fills in the rules
rules: []
```

<https://www.cncf.io/blog/2020/08/28/kubernetes-rbac-101-authorization/>



## RBAC to the Future: Untangling Authorization in Kubernetes

Jimmy Mesta, KSOC

<https://www.youtube.com/watch?v=3bE7o0-1CHY>

```
[*] Started enumerating risky ClusterRoles:
[!][ClusterRole]→ Cluster-pod-creator Has permission to create pods!
[!][ClusterRole]→ Cluster-Secret-reader Has permission to list secrets!
[!][ClusterRole]→ resource-reader Has permission to use get on any resource!
[!][ClusterRole]→ nginx-lb-nginx-ingress Has permission to list secrets!
[!][ClusterRole]→ prometheus-adapter-server-resources Has Admin-Cluster permission!
[!][ClusterRole]→ prometheus-kube-state-metrics Has permission to list secrets!
[!][ClusterRole]→ prometheus-prometheus-oper-operator Has permission to access statefulsets with any verb!
[!][ClusterRole]→ prometheus-prometheus-oper-operator Has permission to list secrets!
[!][ClusterRole]→ prometheus-prometheus-oper-operator Has permission to access secrets with any verb!
[*] Started enumerating risky Roles:
[!][Role]→ nginx-lb-nginx-ingress Has permission to list secrets!
[!][Role]→ kubesystem-pod-creator Has permission to create pods!
[!][Role]→ default-admin Has Admin-Cluster permission!
[!][Role]→ res-reader Has permission to use get on any resource!
[!][Role]→ Random-user Has permission to use get on any resource!
[!][Role]→ local-secret-reader Has permission to list secrets!
[*] Started enumerating risky ClusterRoleBinding:
[!][ClusterRoleBinding]→ nginx-lb-nginx-ingress is bound to nginx-lb-nginx-ingress ServiceAccount.
[!][ClusterRoleBinding]→ sa1-resources is bound to sa1 ServiceAccount.
[!][ClusterRoleBinding]→ secret-reader is bound to sa-secret-reader ServiceAccount.
[!][ClusterRoleBinding]→ sa-pod-creator is bound to sa-pod-creator ServiceAccount.
[!][ClusterRoleBinding]→ prometheus-adapter-hpa-controller is bound to prometheus-adapter ServiceAccount.
[!][ClusterRoleBinding]→ prometheus-kube-state-metrics is bound to prometheus-kube-state-metrics ServiceAccount.
[!][ClusterRoleBinding]→ prometheus-prometheus-oper-operator is bound to prometheus-prometheus-oper-operator ServiceAccount.
[*] Started enumerating risky RoleBinding:
[!][RoleBinding]→ nginx-lb-nginx-ingress is bound to nginx-lb-nginx-ingress ServiceAccount.
[!][RoleBinding]→ local-secret is bound to kubesystem-secret-reader ServiceAccount.
```

<https://github.com/cyberark/kubernetes-rbac-audit>

← Post



Ian Coldwater 📦💥  
@IanColdwater

We are all made of stars, but your RBAC shouldn't be

2:08 AM · Feb 8, 2020

...



35

246

1,382

26



# K04 - Lack of Centralized Policy Enforcement



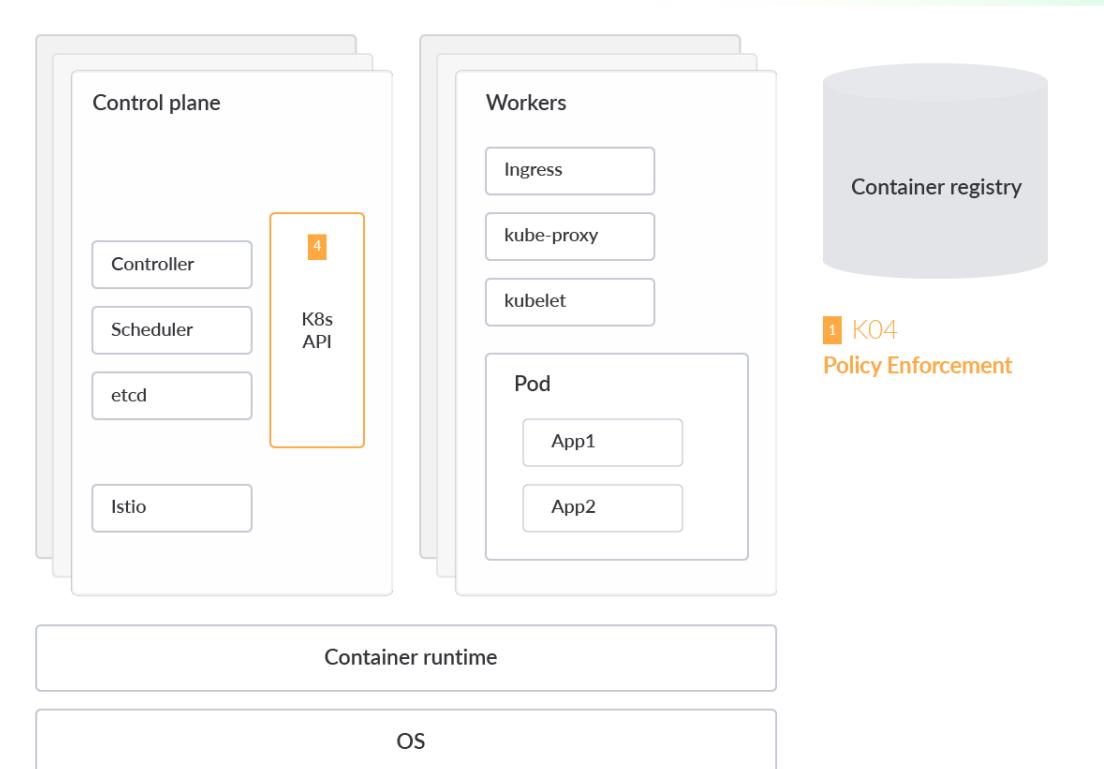
The **Admission Configuration** resource needs to be managed individually on each cluster.



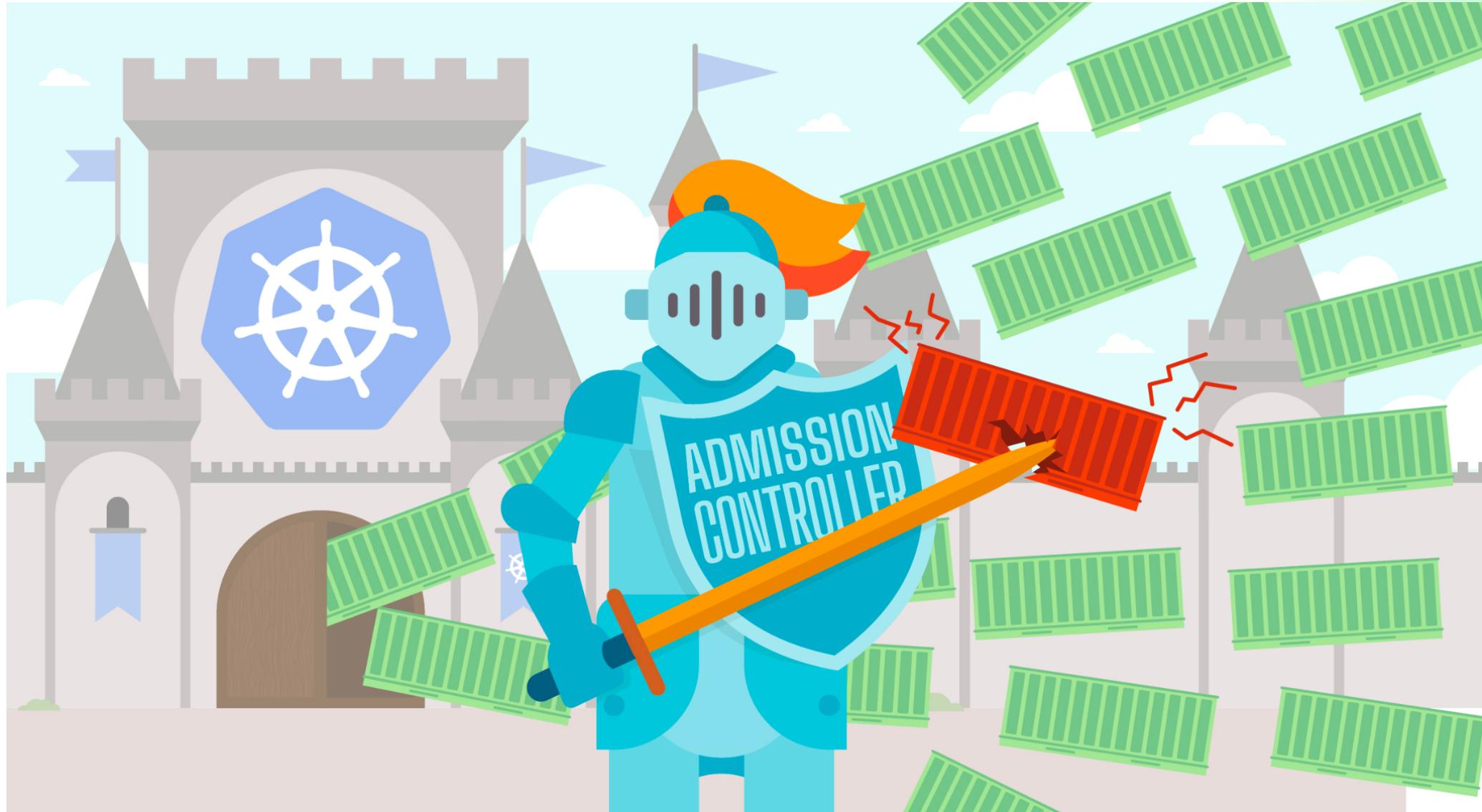
**Kube-Mgmt** manages policies & data of OPA instances within Kubernetes – instead of managing admission controllers individually.



**Falco** can source the K8s audit logs to show examples of private credentials that might be exposed in ConfigMaps in any Namespace.



# Lack of Policies



# K05 - Inadequate Logging and Monitoring



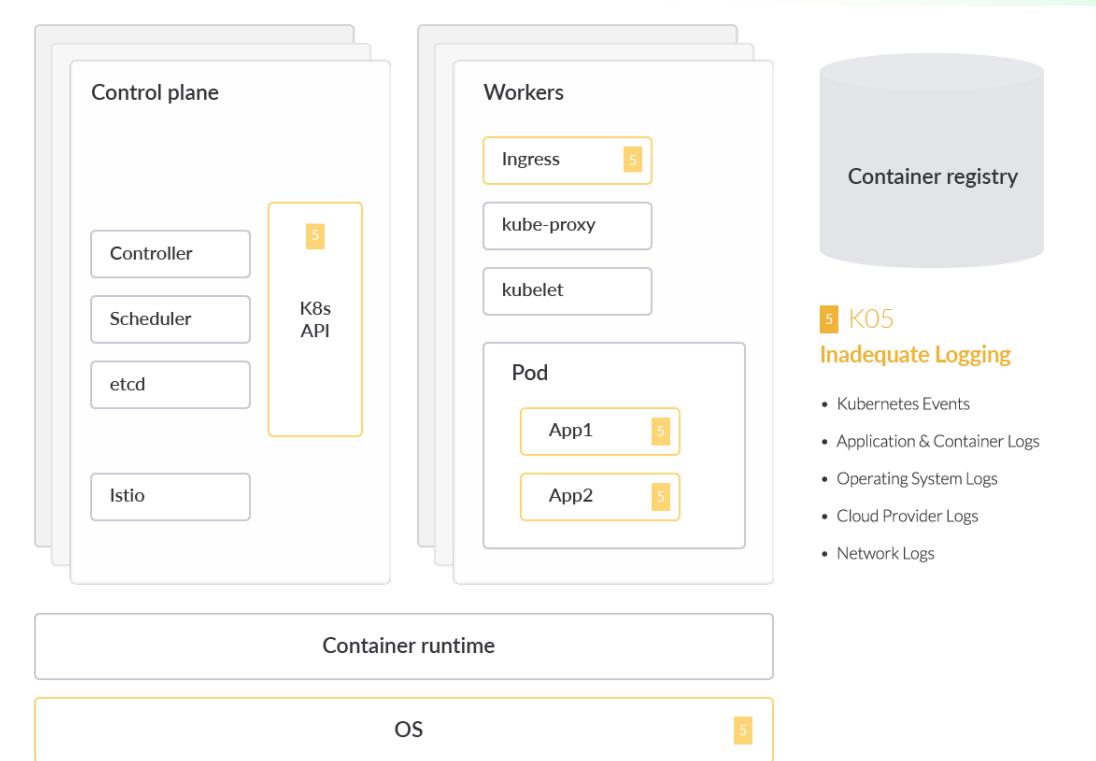
**Prometheus** was designed with the intention of monitoring cloud-native apps.



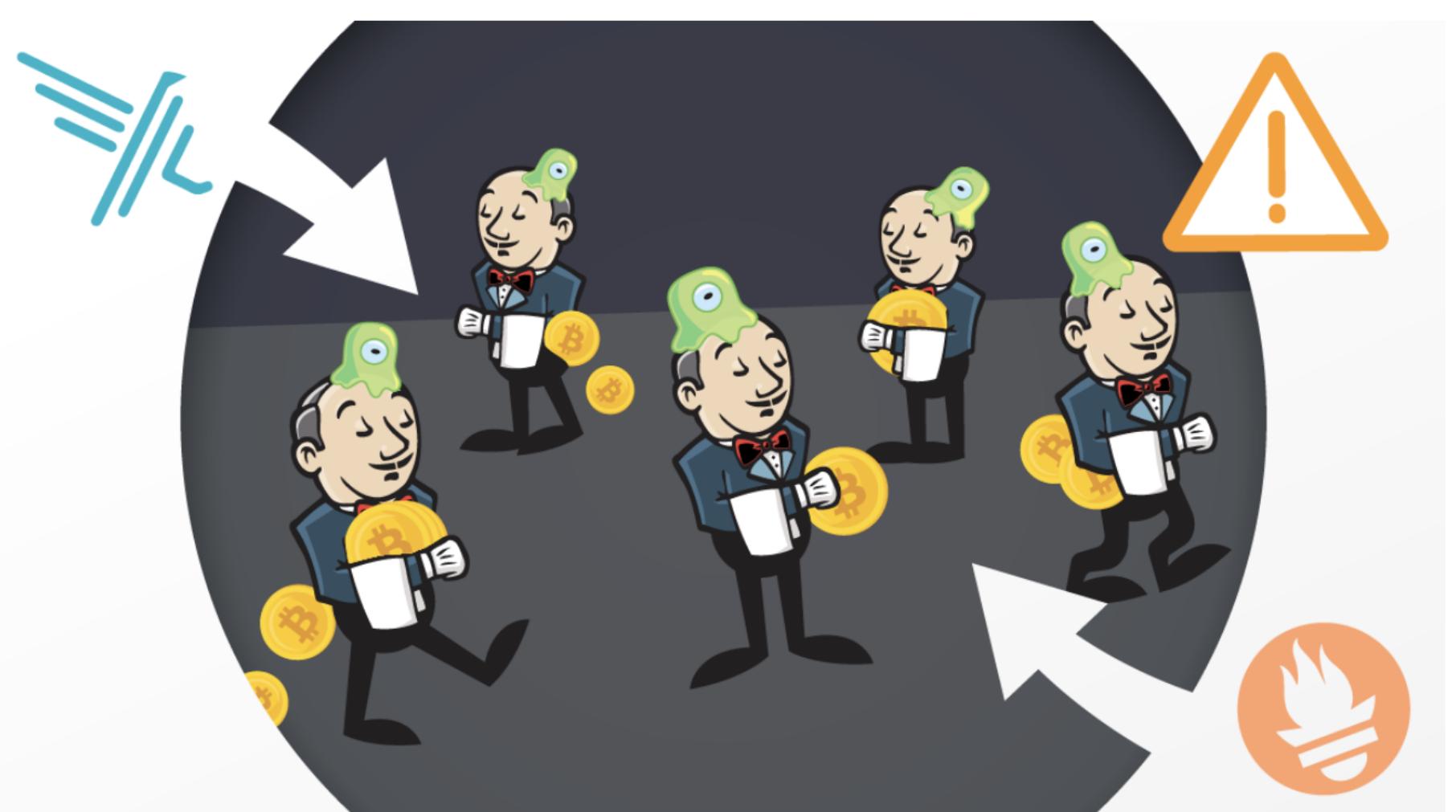
**Grafana** allows you to query, visualize, alert on, and understand your metrics no matter where they are stored.



**Falco** detects threats at runtime by observing the behavior of your applications and containers. It extends threat detection to Kubernetes via its plugin architecture.



# DEMO Falco



# K06 - Broken Authentication Mechanisms



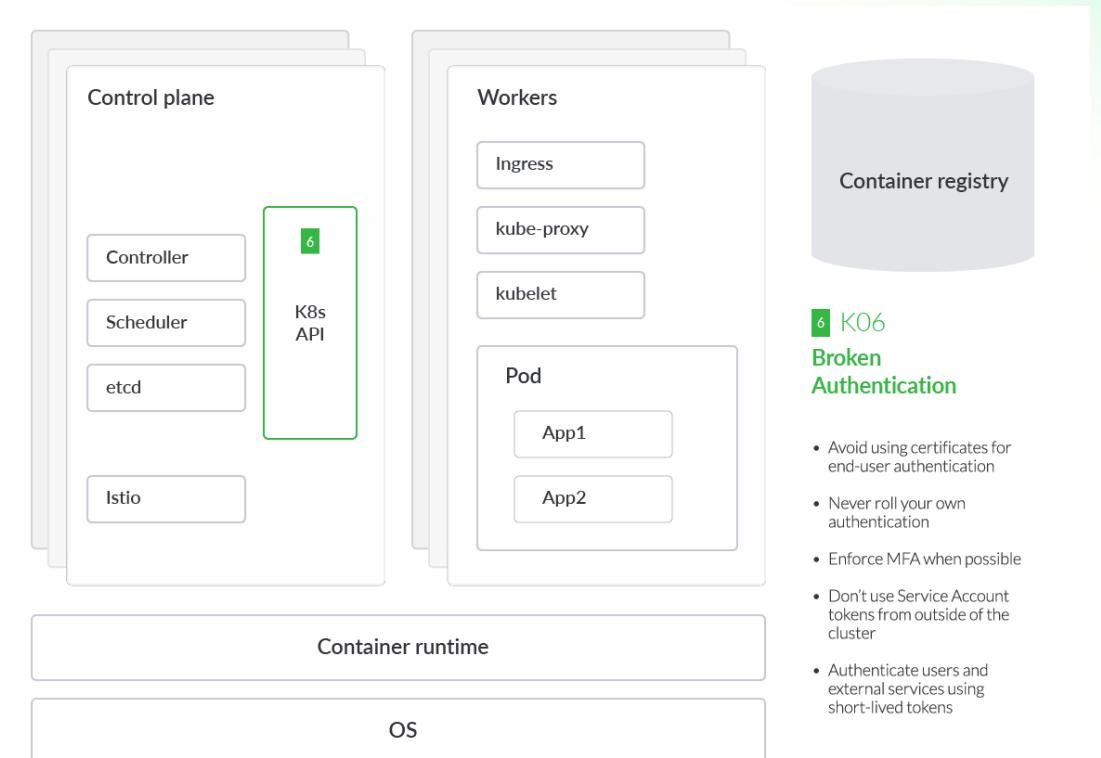
**Enforce MFA** where possible



**Enforce RBAC Restrictions** for ServiceAccounts where possible



**Enforce Passwords** on public-facing resources like Kubernetes dashboards



# Shodan / K8s

## Tesla cloud resources are hacked to run cryptocurrency-mining malware

Crooks find poorly secured access credentials, use them to install stealth miner.

DAN GOODIN - 2/20/2018, 8:21 PM

2/20/2018,

A screenshot of a web-based Kubernetes interface. The URL in the address bar is `https://[REDACTED]/#/secret/default/aws-s3-credentials?namespace=default`. The page title is "kubernetes". The main navigation menu has "Config and storage" selected, followed by "Secrets" and "aws-s3-credentials". On the left, there's a sidebar with "Namespace" dropdown set to "default", and links for "Overview", "Workloads", "Daemon Sets", "Deployments", "Jobs", "Pods", "Replica Sets", "Replication Controllers", and "Stateful Sets". The main content area is titled "Details" and shows the following information:

Name	Namespace	Creation time	Type
aws-s3-credentials	default	2017-10-12T22:29	Opaque

Below the details section is a "Data" section containing two entries:

- aws-s3-access-key-id: [REDACTED]
- aws-s3-secret-access-key: [REDACTED]

# Shodan / K8s

Tesla  
crypt

Crooks find

DAN GOODIN - 2

Not Secure | https://[REDACTED] #!/secret/default/aws-s3-credentials?namespace=default

SHODAN Explore Downloads Pricing View Report View on Map

TOTAL RESULTS 3,685

TOP COUNTRIES

Country	Count
United States	1,580
Canada	499
China	312
Ireland	299
India	203
More...	

TOP PORTS

Port	Count
443	2,544
80	630
9090	226
8443	156
8000	46
More...	

TOP ORGANIZATIONS

Organization	Count
Amazon Technologies Inc.	1,085
Amazon Data Services Canada	487
Amazon.com, Inc.	277
Amazon Data Services Ireland Limited	214
Amazon Data Services NoVa	213

**Kubernetes Dashboard**   
35.182.81.163  
ec2-35-182-81-163.ca-central-1.compute.amazonaws.com  
Amazon Data Services Canada  
Canada, Montreal  
cloud

**SSL Certificate**   
Issued By: Amazon RSA 2048 M03  
Issued To: \*.el01.na4.atomx.nanostring.com  
Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 200 OK  
Date: Thu, 21 Sep 2023 09:29:55 GMT  
Content-Type: text/html; charset=utf-8  
Content-Length: 1412  
Connection: keep-alive  
Accept-Ranges: bytes  
Cache-Control: no-cache, no-store, must-revalidate  
Last-Modified: Fri, 16 Sep 2022 11:49:34 GMT

**Kubernetes Dashboard**   
3.109.23.225  
ec2-3-109-23-225.ap-south-1.compute.amazonaws.com  
Amazon Data Services India  
India, Mumbai  
cloud

**SSL Certificate**   
Issued By: Amazon RSA 2048 M03  
Issued To: \*.  
Supported SSL Versions: TLSv1.2, TLSv1.3

HTTP/1.1 200 OK  
Accept-Ranges: bytes  
Cache-Control: no-cache, no-store, must-revalidate  
Content-Length: 1412  
Content-Type: text/html; charset=utf-8  
Last-Modified: Thu, 03 Feb 2022 15:57:38 GMT  
Date: Thu, 21 Sep 2023 09:22:37 GMT

**Kubernetes Dashboard**   
15.222.98.196  
ec2-15-222-98-196.ca-central-1.compute.amazonaws.com  
Amazon Data Services Canada  
Canada, Montréal  
cloud

**SSL Certificate**   
Issued By: Amazon RSA 2048 M02  
Issued To: \*.mdaac.na3.atomx.nanostring.com  
Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 200 OK  
Date: Thu, 21 Sep 2023 09:21:23 GMT  
Content-Type: text/html; charset=utf-8  
Content-Length: 1412  
Connection: keep-alive  
Accept-Ranges: bytes  
Cache-Control: no-cache, no-store, must-revalidate  
Last-Modified: Fri, 16 Sep 2022 11:49:34 GMT

# K07 - Network Segmentation Controls



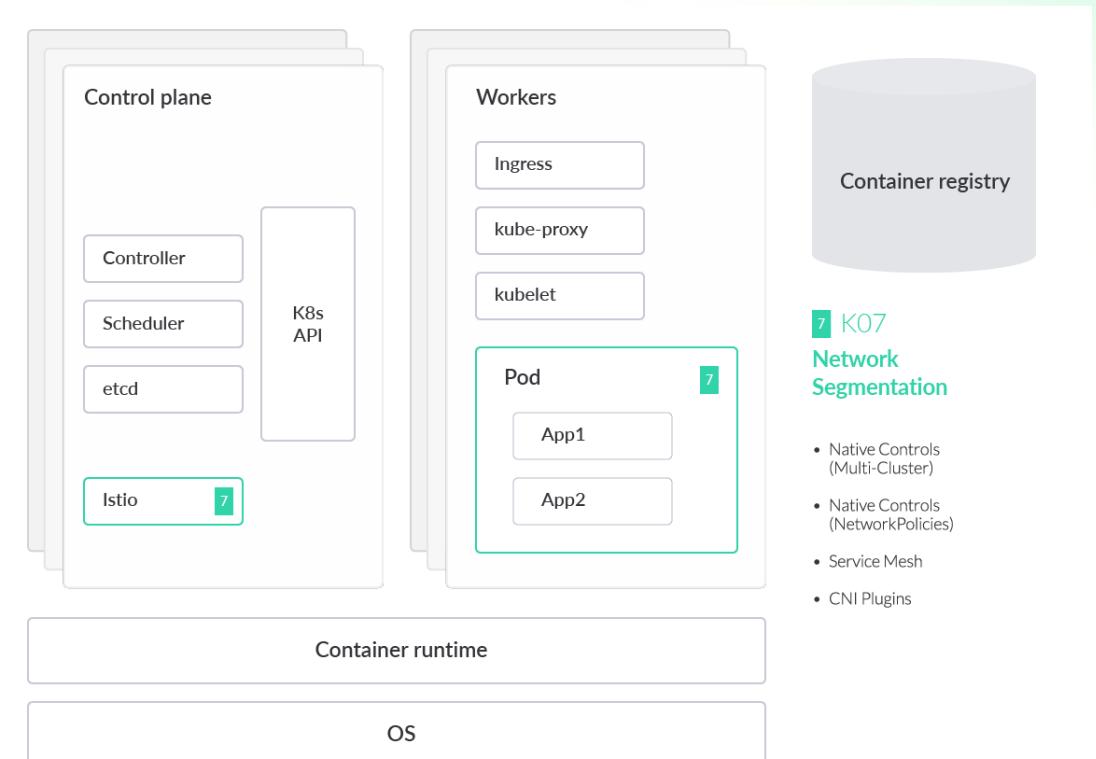
**Istio** provides a service mesh solution.



**CNI** like Calico & Cilium are primarily focused on L3/L4 (Network) enforcement.



**CNCF** says that the majority of Kubecon participants (65%) run or plan to run between 2 and 10 Kubernetes clusters on a service mesh

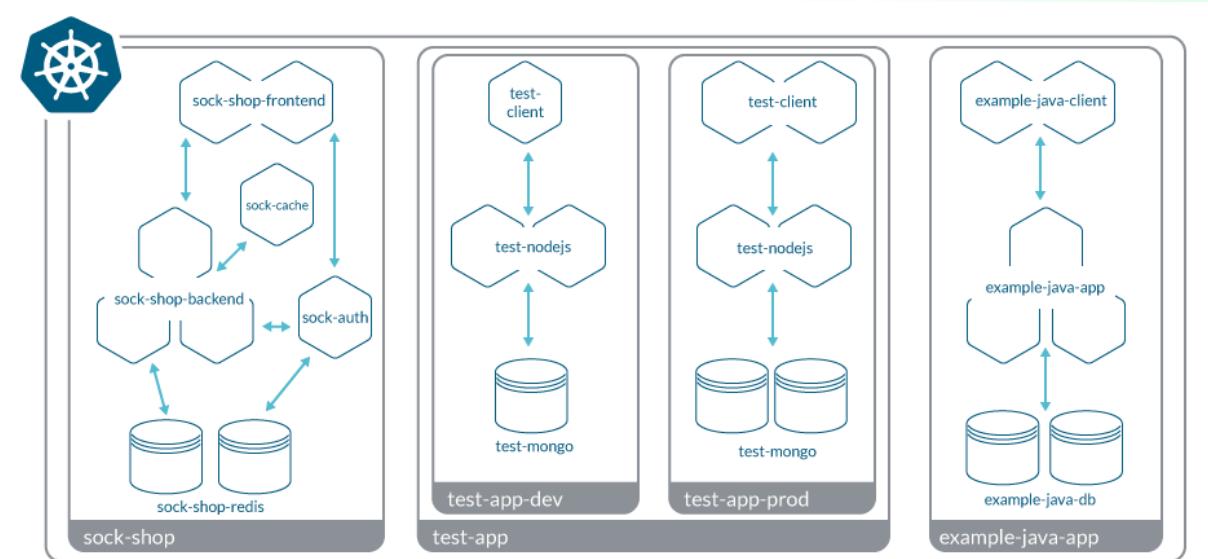
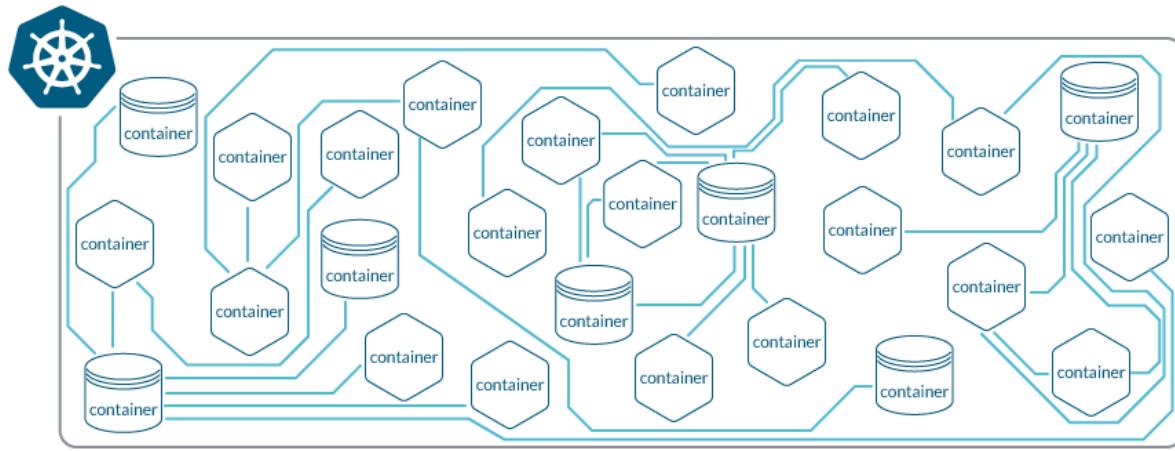


Source: [https://www.cncf.io/wp-content/uploads/2022/05/CNCF\\_Service\\_Mesh\\_MicroSurvey\\_Final.pdf](https://www.cncf.io/wp-content/uploads/2022/05/CNCF_Service_Mesh_MicroSurvey_Final.pdf)

## 7 K07 Network Segmentation

- Native Controls (Multi-Cluster)
- Native Controls (NetworkPolicies)
- Service Mesh
- CNI Plugins

# Service meshes, network policies deny by default, mTLS with service meshes...



Istio



# K08 - Secrets Management Failures



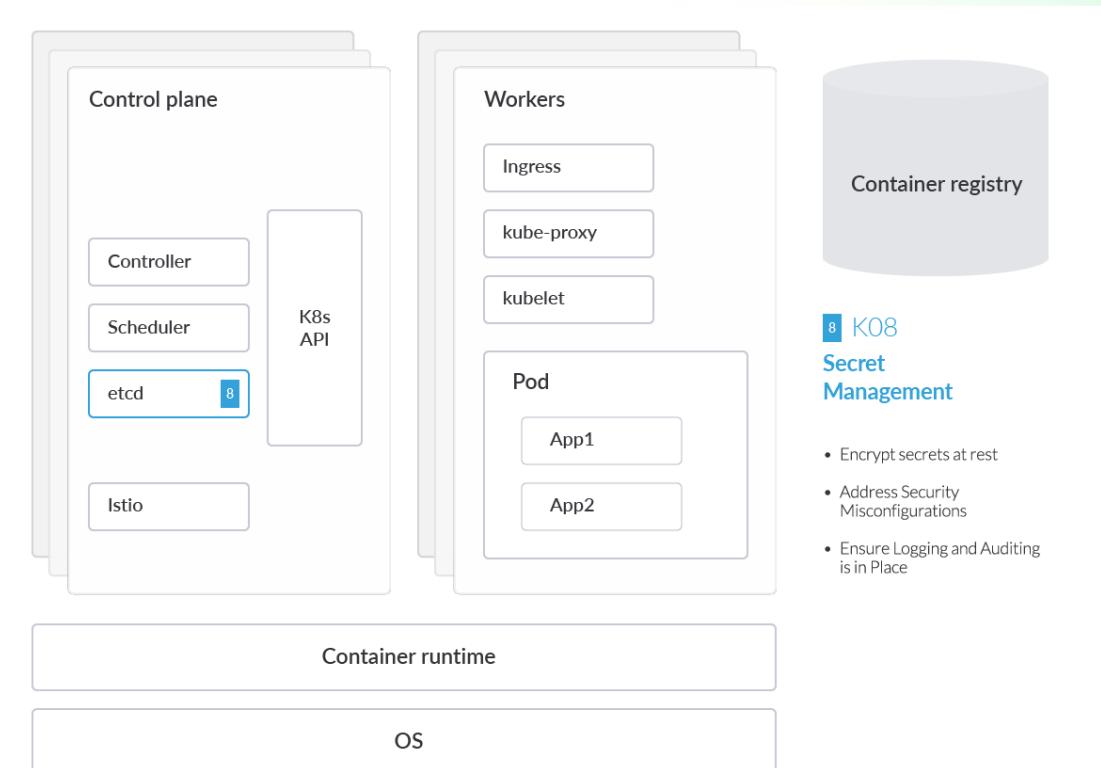
As of v.1.7, Kubernetes supports the **Encrypting of Secrets at-rest** for etcd.



**Avoid credentials sharing** and where possible enforce the principle of least privilege on Service Accounts



**Falco** can stream the standard output (stdout) of alerts to **Fluentd** or **Logstash**, allowing teams such as platform engineering or security operations to capture event data easily from Kubernetes.



## DEMO TIME

- Quick demo showing k8s secrets inside cluster are simply base64

```
* base64-is-not-encryption master ✓ kubectl create secret generic demo --from-literal=password=encrapption  
secret "demo" created  
→ base64-is-not-encryption master ✓ kubectl exec -it -n kube-system etcd-minik|
```

# K09 - Misconfigured Cluster Components



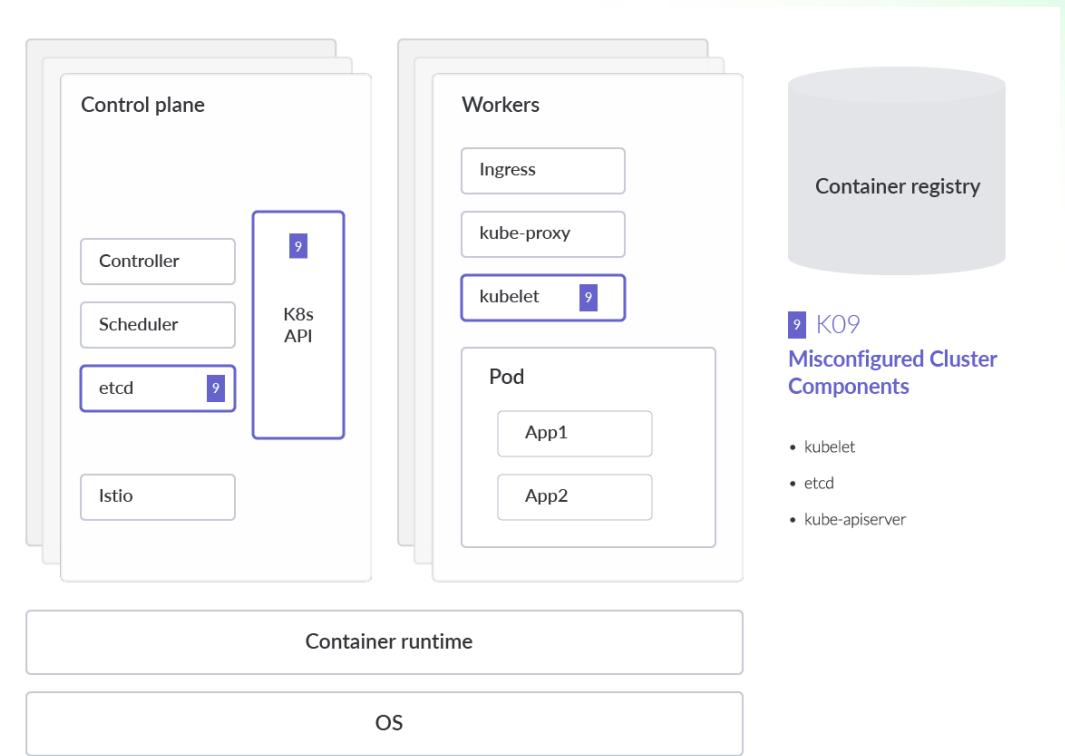
We strongly recommend regularly *backing up etcd* data to avoid data loss.



It is also important to regularly *rotate TLS certificates* for the **Kube-API**, especially for long-lived Kubernetes clusters.



One of the riskiest misconfigurations is the ***Anonymous Authentication*** setting in **Kubelet**, which allows non-authenticated requests to the Kubelet.



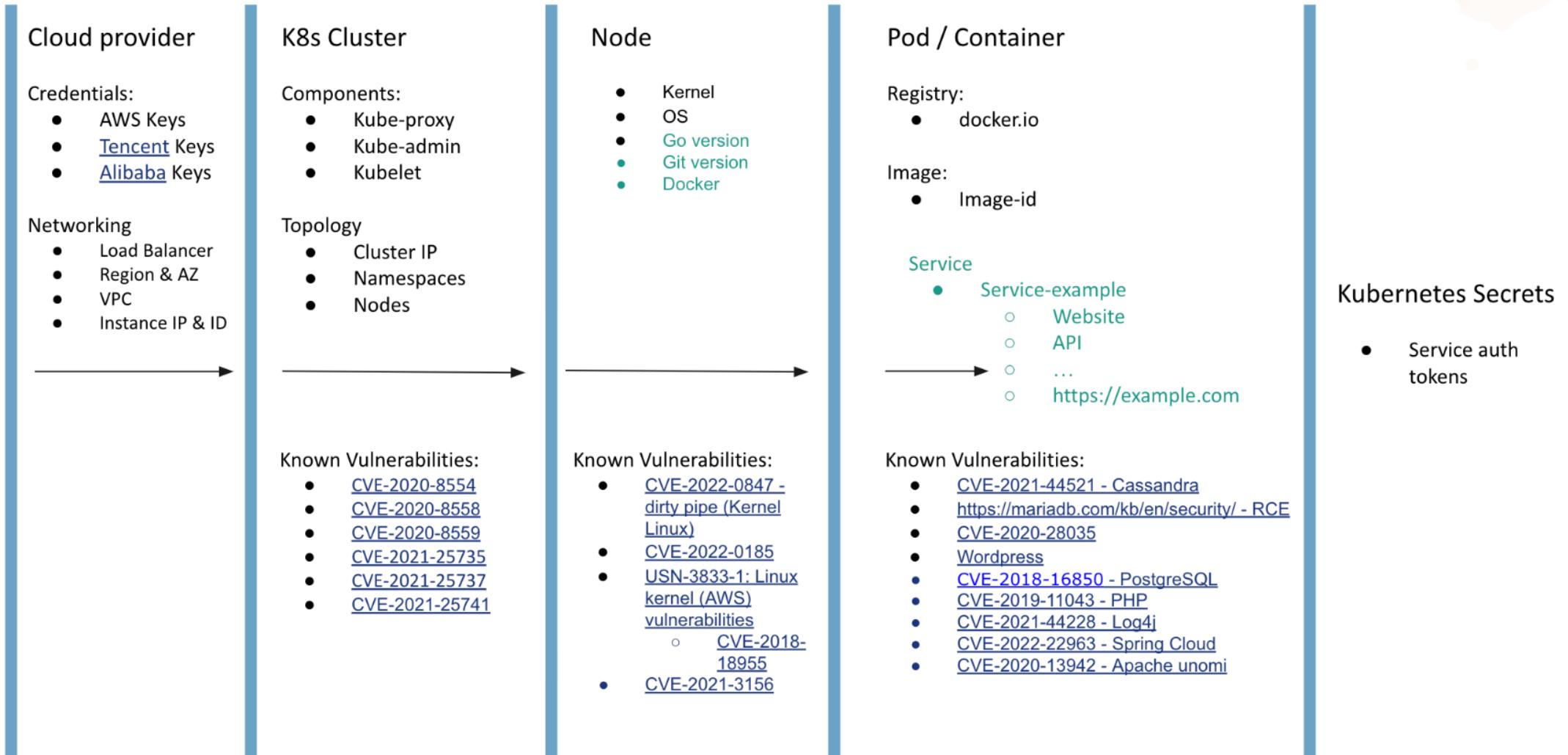
# How Attackers Use Exposed Prometheus Server to Exploit Kubernetes Clusters

Miguel Hernández & David de Torres, Sysdig

[https://www.youtube.com/watch?v=5cbbm\\_L6n7w](https://www.youtube.com/watch?v=5cbbm_L6n7w)



HackK8s Cluster Any%	3
	<b>1:58.92</b>
Gathering info - Prometheus	<b>-1:23</b> 0:32.9
Initial access - T1195	<b>-1:24</b> 0:50.0
Level Up - Elevation Privileges	<b>-1:23</b> 1:06.9
Gain Persistence	<b>-1:58</b> 1:18.4
Leak Secrets	<b>-2:10</b> 1:26.9
Remove evidences	<b>-2:08</b> 1:42.6
\$\$\$\$\$\$\$	<b>-2:11</b> 1:58.9



# K10 - Outdated & Vulnerable K8s Components



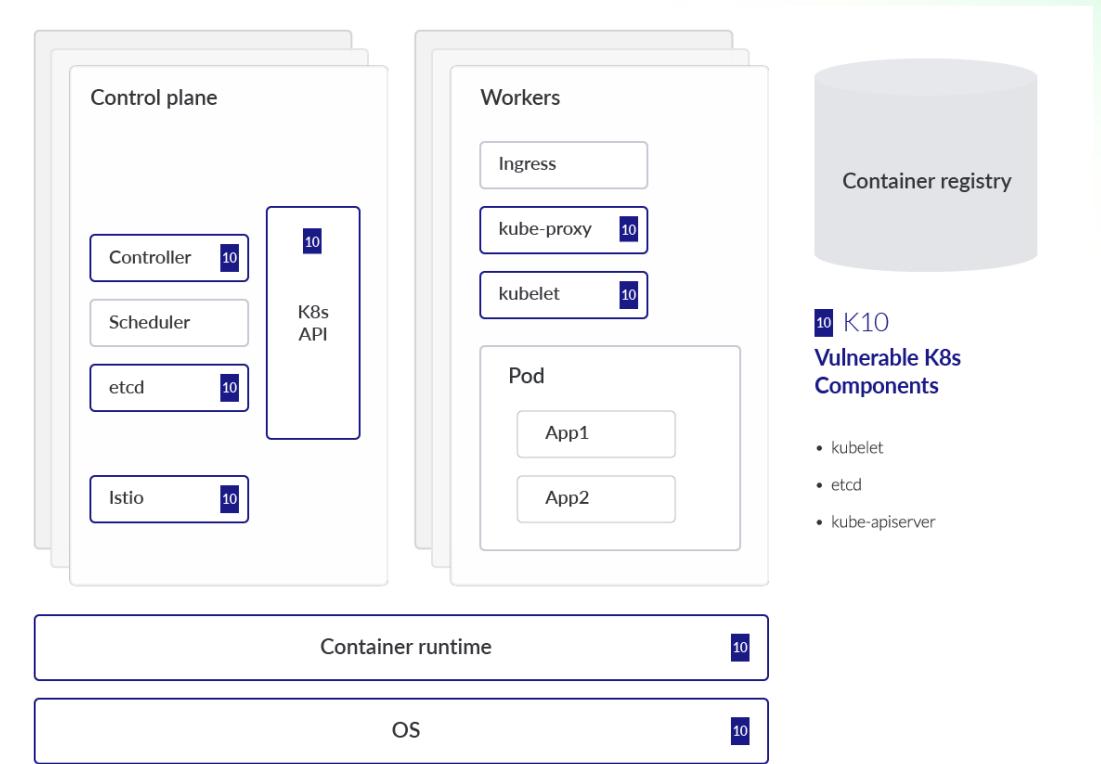
**CVE-2018-18264** – Privilege escalation through Kubernetes dashboard



**CVE-2020-8554** – Unpatched Man-In-The-Middle (MITM) Attack in K8s



**CVE-2019-11246** – High-severity vulnerability affecting kubectl tool. If exploited, it could lead to a directory traversal.



# Kubernetes CVE Feed - DEMO

[Kubernetes Documentation](#) / [Reference](#) / [Kubernetes Issues and Security](#) / [CVE feed](#)

## Official CVE Feed

FEATURE STATE: [Kubernetes v1.27](#) [beta]

This is a community maintained list of official CVEs announced by the Kubernetes Security Response Committee. See [Kubernetes Security and Disclosure Information](#) for more details.

The Kubernetes project publishes a programmatically accessible feed of published security issues in [JSON feed](#) and [RSS feed](#) formats. You can access it by executing the following commands:

[JSON feed](#)

[RSS feed](#)

[Link to JSON format](#)

```
curl -Ls https://k8s.io/docs/reference/issues-security/official-cve-feed/index.json
```

Official Kubernetes CVE List (last updated: 21 Sep 2023 01:28:05 UTC)

CVE ID	Issue Summary	CVE GitHub Issue URL
<a href="#">CVE-2023-2431</a>	Bypass of seccomp profile enforcement	<a href="#">#118690</a>
<a href="#">CVE-2023-2727, CVE-2023-2728</a>	Bypassing policies imposed by the ImagePolicyWebhook and bypassing mountable secrets policy imposed by the ServiceAccount admission plugin	<a href="#">#118640</a>
<a href="#">CVE-2023-2878</a>	secrets-store-csi-driver discloses service account tokens in logs	<a href="#">#118419</a>
<a href="#">CVE-2022-3294</a>	Node address isn't always verified when proxying	<a href="#">#113757</a>
<a href="#">CVE-2022-3162</a>	Unauthorized read of Custom Resources	<a href="#">#113756</a>
<a href="#">CVE-2022-3172</a>	Aggregated API server can cause clients to be redirected (SSRF)	<a href="#">#112513</a>
<a href="#">CVE-2021-25749</a>	'runAsNonRoot' logic bypass for Windows containers	<a href="#">#112192</a>
<a href="#">CVE-2021-25741</a>	Symlink Exchange Can Allow Host Filesystem Access	<a href="#">#104980</a>
<a href="#">CVE-2021-25737</a>	Holes in EndpointSlice Validation Enable Host Network Hijack	<a href="#">#102106</a>
<a href="#">CVE-2021-3121</a>	Processes may panic upon receipt of malicious protobuf messages	<a href="#">#101435</a>
<a href="#">CVE-2021-25735</a>	Validating Admission Webhook does not observe some previous fields	<a href="#">#100096</a>
<a href="#">CVE-2020-8554</a>	Man in the middle using LoadBalancer or ExternalIPs	<a href="#">#97076</a>
<a href="#">CVE-2020-8566</a>	Ceph RBD adminSecrets exposed in logs when loglevel >= 4	<a href="#">#95624</a>
<a href="#">CVE-2020-8565</a>	Incomplete fix for CVE-2019-11250 allows for token leak in logs when logLevel >= 9	<a href="#">#95623</a>
<a href="#">CVE-2020-8564</a>	Docker config secrets leaked when file is malformed and log level >= 4	<a href="#">#95622</a>
<a href="#">CVE-2020-8563</a>	Secret leaks in kube-controller-manager when using vSphere provider	<a href="#">#95621</a>
<a href="#">CVE-2020-8557</a>	Node disk DOS by writing to container /etc/hosts	<a href="#">#93032</a>
<a href="#">CVE-2020-8559</a>	Privilege escalation from compromised node to cluster	<a href="#">#92914</a>
<a href="#">CVE-2020-8558</a>	Node setting allows for neighboring hosts to bypass localhost boundary	<a href="#">#92315</a>
<a href="#">CVE-2020-8555</a>	Half-Blind SSRF in kube-controller-manager	<a href="#">#91542</a>
<a href="#">CVE-2020-10749</a>	IPv4 only clusters susceptible to MitM attacks via IPv6 rogue router advertisements	<a href="#">#91507</a>
<a href="#">CVE-2019-11254</a>	kube-apiserver Denial of Service vulnerability from malicious YAML payloads	<a href="#">#89535</a>
<a href="#">CVE-2020-8552</a>	apiserver DoS (oom)	<a href="#">#89378</a>

<https://kubernetes.io/docs/reference/issues-security/official-cve-feed/>

# Conclusions

# Take aways

- ❑ Understand Kubernetes security risks.
- ❑ Which tools do we have available to audit and secure our systems.
- ❑ DIY.

# Thank you!