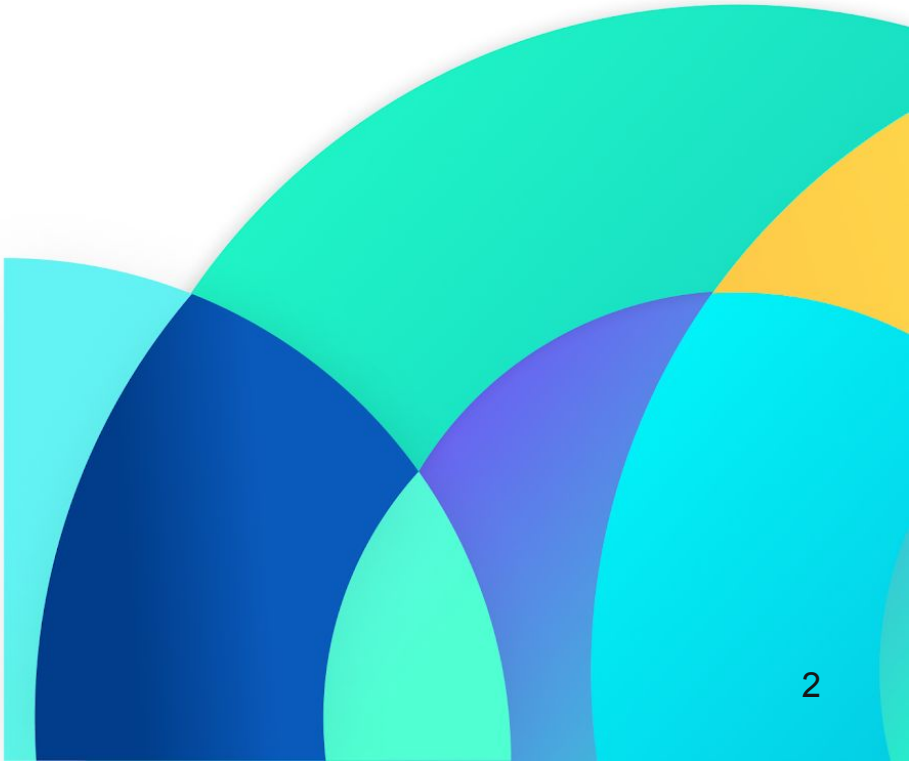
Dig deeper into OWASP Kubernetes

Miguel Hernández
Threat Research Engineer
Sysdig
@miguelhzbz

Daniel Simionato
Technical Marketing Manager
Sysdig
@weseven

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?



Poll:

What's your level of experience with securing Kubernetes?

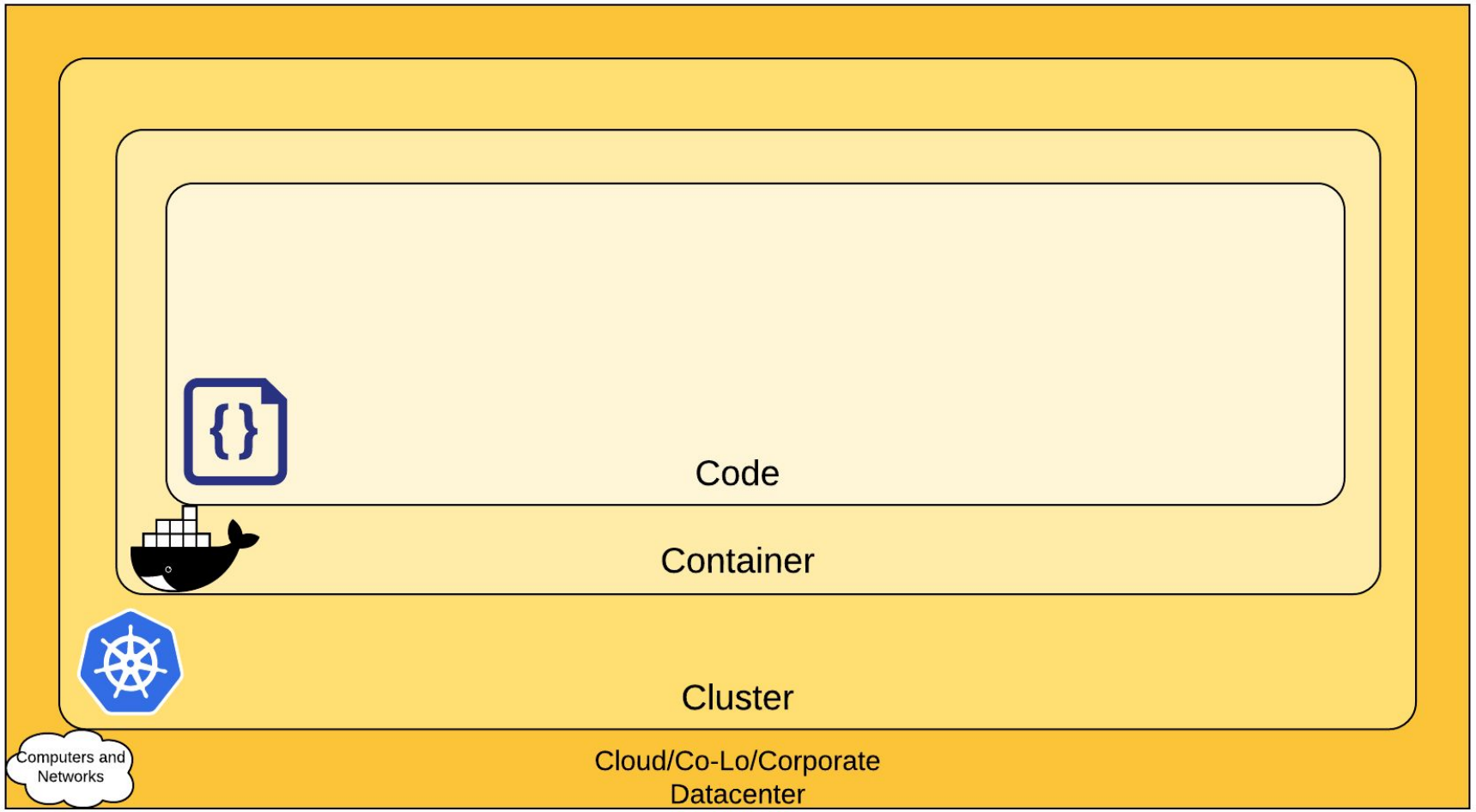
- What's Kubernetes again?
- I'm an early learner.
- I can get the job done.
- I'm a guru!

1. What is the OWASP Kubernetes Top 10?

Why do we care?

- Kubernetes is the defacto standard for container orchestration
- Organizations need security standards and guidance

The 4C's of Cloud Native security



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

Kubernetes CIS Benchmark

Recent versions available for CIS Benchmark:

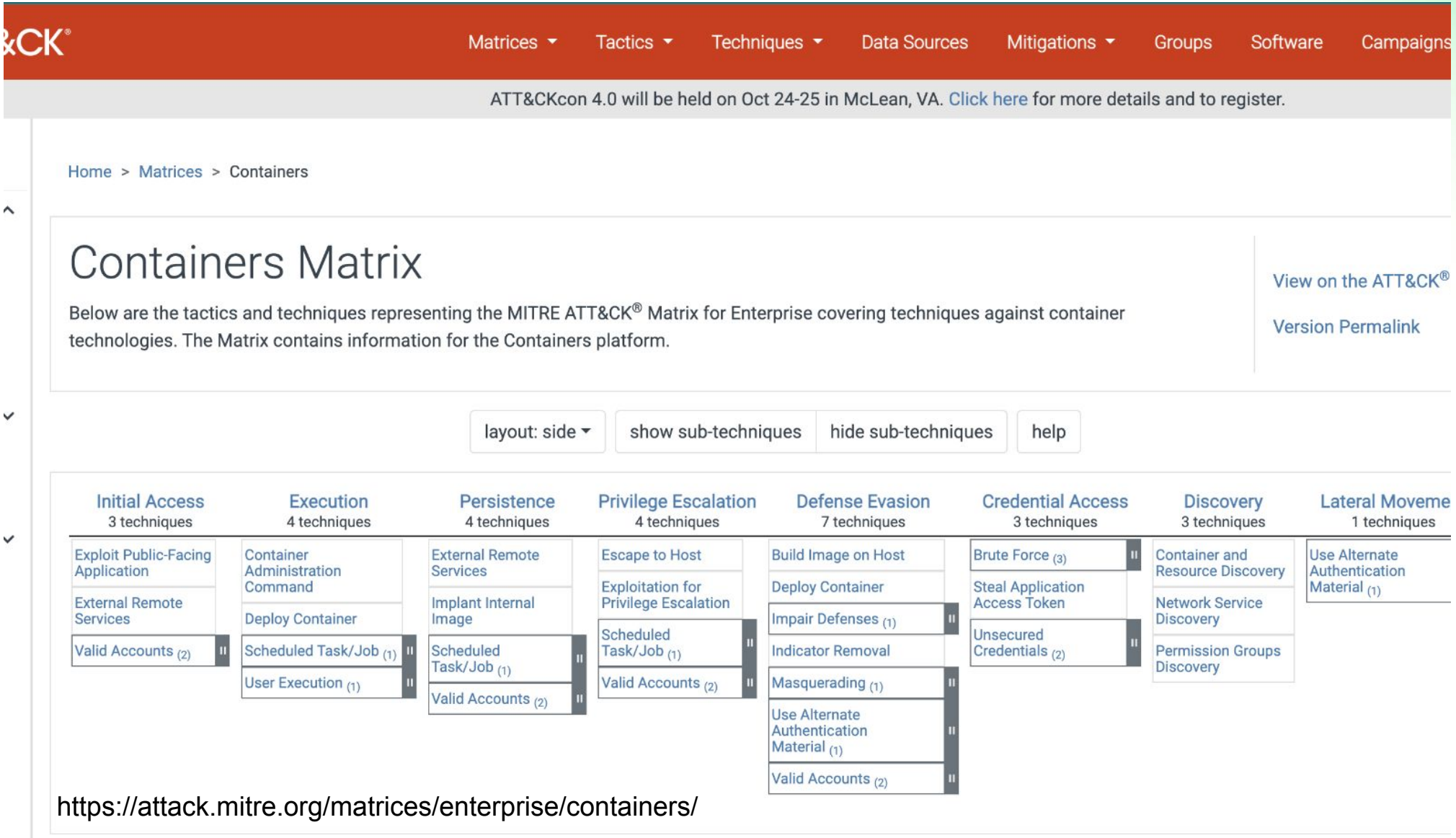
- Alibaba Cloud Container Service For Kubernetes (ACK) (1.0.0)
- Amazon Elastic Kubernetes Service (EKS) (1.3.0)
- Azure Kubernetes Service (AKS) (1.3.0)
- Google Kubernetes Engine (GKE) (1.4.0)
- Kubernetes (1.7.1)
- Kubernetes V1.24 (1.0.0)
- Kubernetes V1.23 (1.0.1)
- Kubernetes V1.20 (1.0.1)
- Oracle 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

Why do we care?

- Kubernetes is the defacto standard for container orchestration
- Organizations need security standards and guidance
- **MITRE ATT&CK for Containers isn't specific to Kubernetes**
- **Fragmentation results with vendor interpretations of ATT&CK**

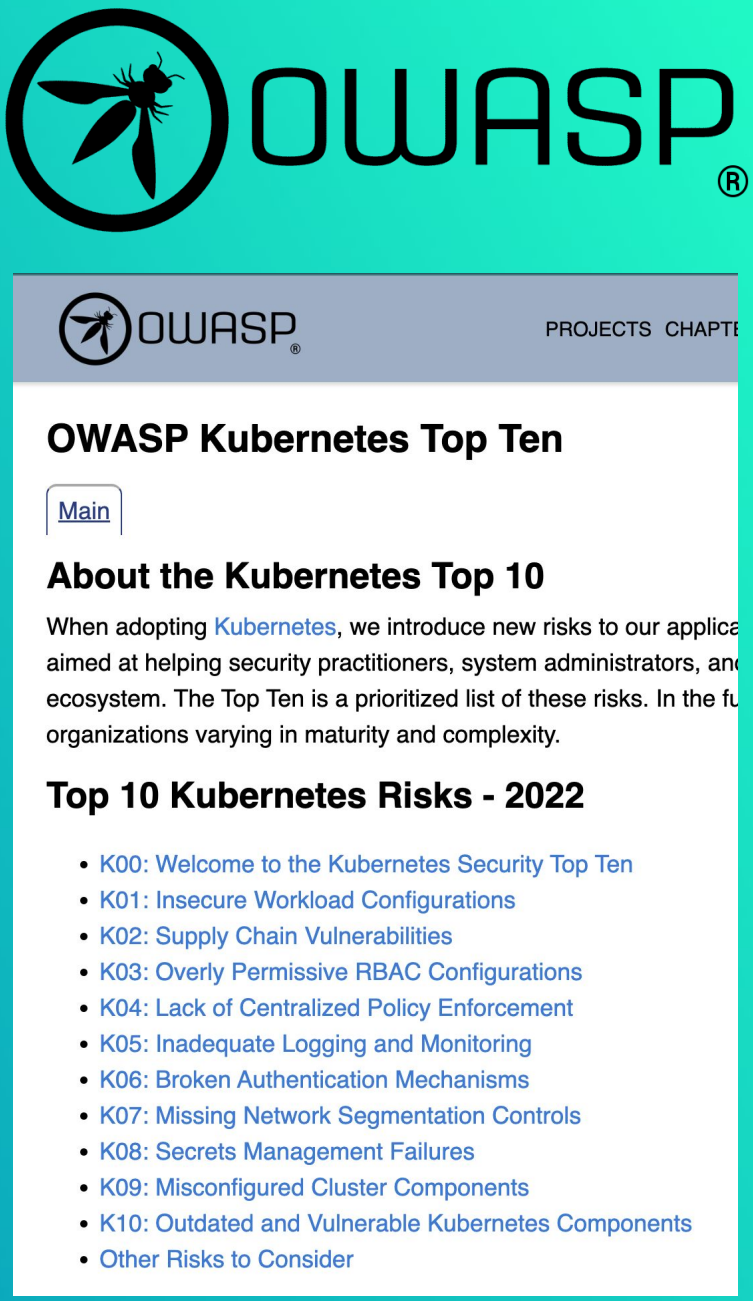
MITRE ATT&CK Containers Matrix



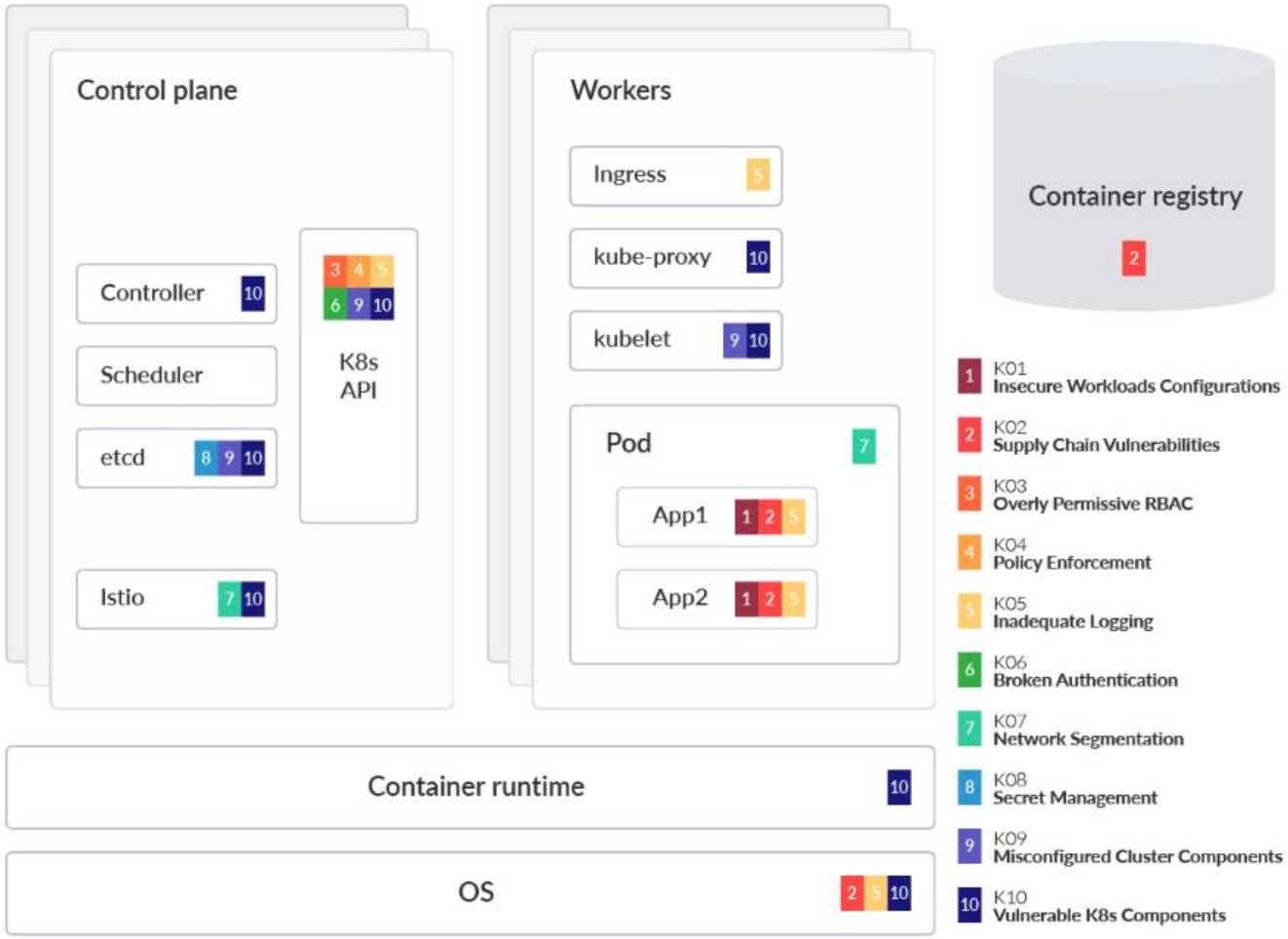
https://attack.mitre.org/matrices/enterprise/containers/

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/



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

K09 - Misconfigured Cluster Components

K10 - Vulnerable K8s Components

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

2. Why are Kubernetes risks so concerning?

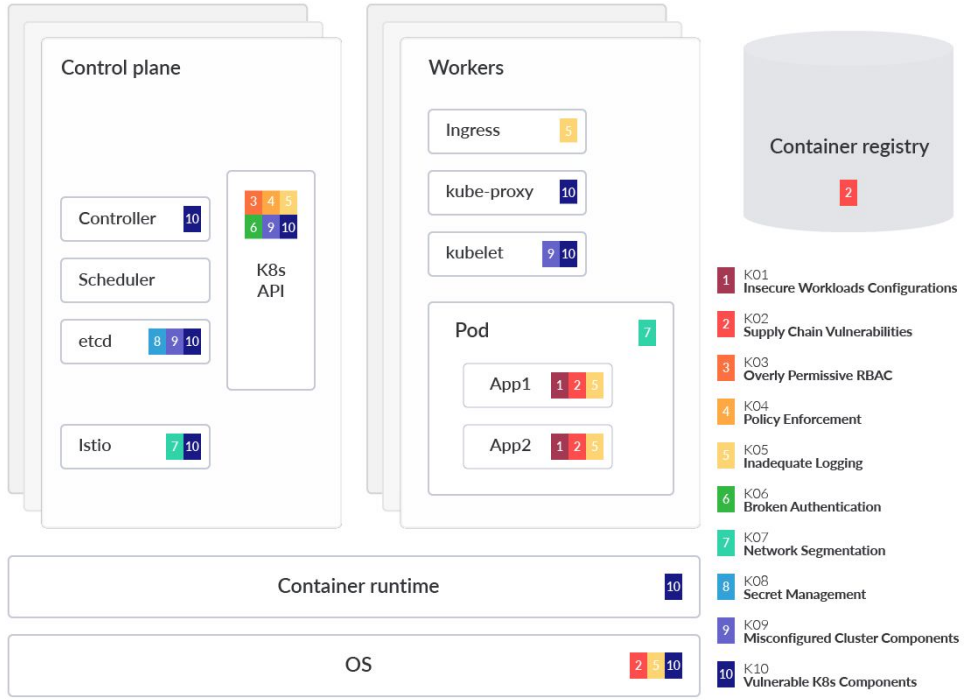
Complexity increases through added abstractions

Managed K8s providers own external connections

Kubernetes is often exposed to the outside world

You need to control access to resources your team uses

You need to detect unusual activity in ephemeral workloads



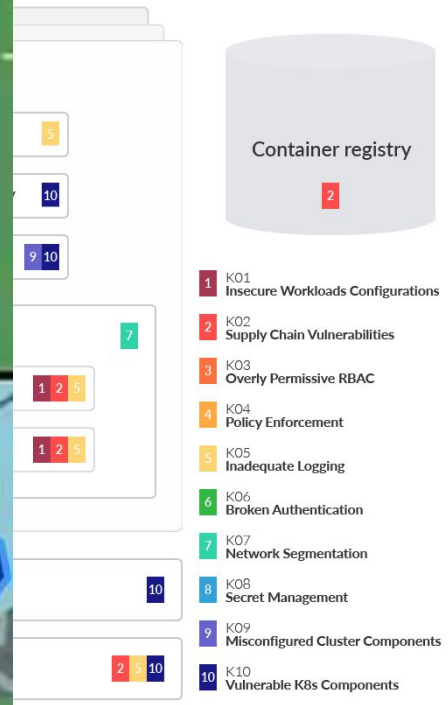
Complexity incr ons

Managed K8s pro
connections

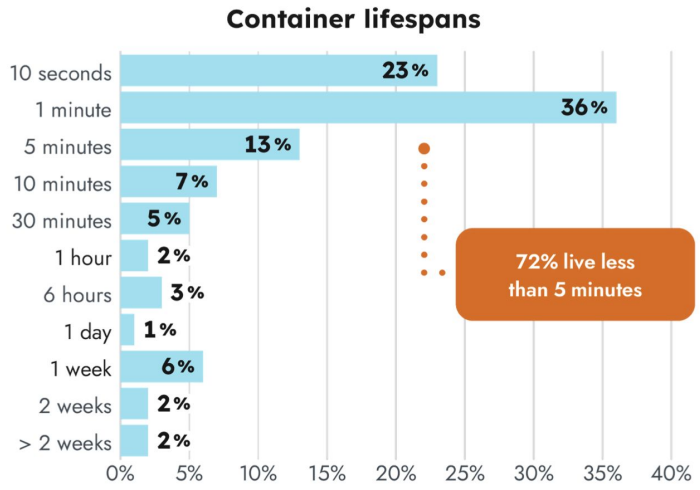
Kubernetes is ofte
world

You need to contr
team uses

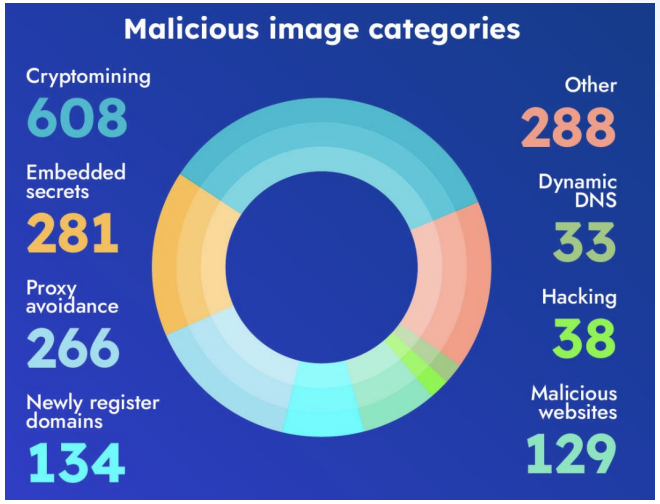
You need to detec
ephemeral worklo



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

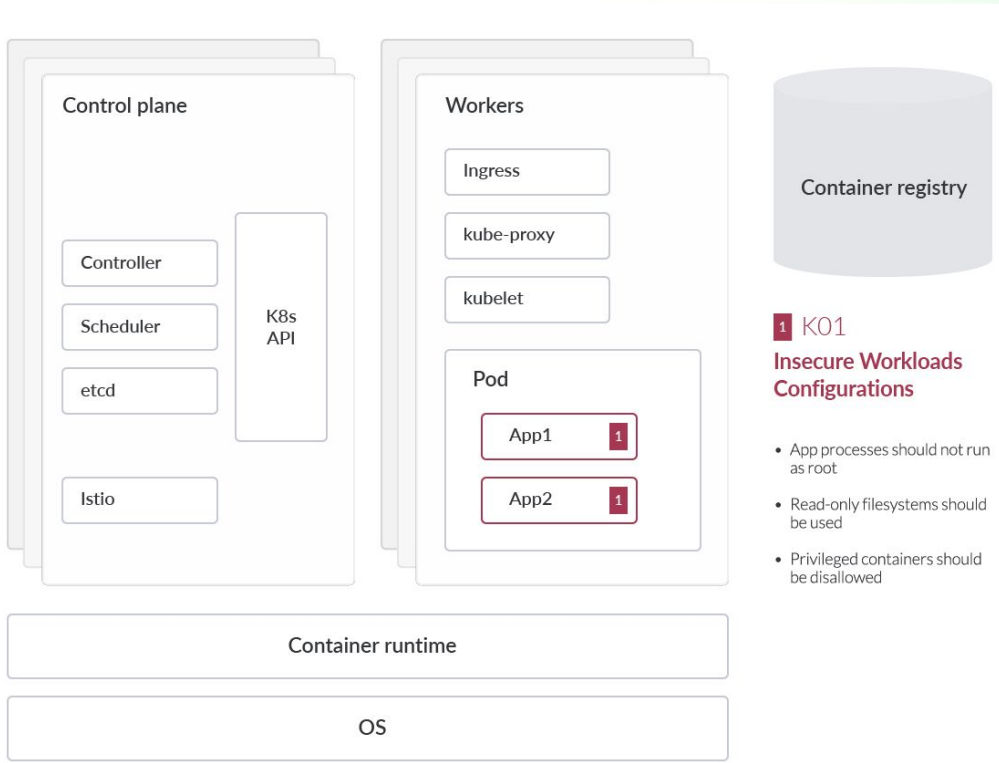
3. What are the common security risks?

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

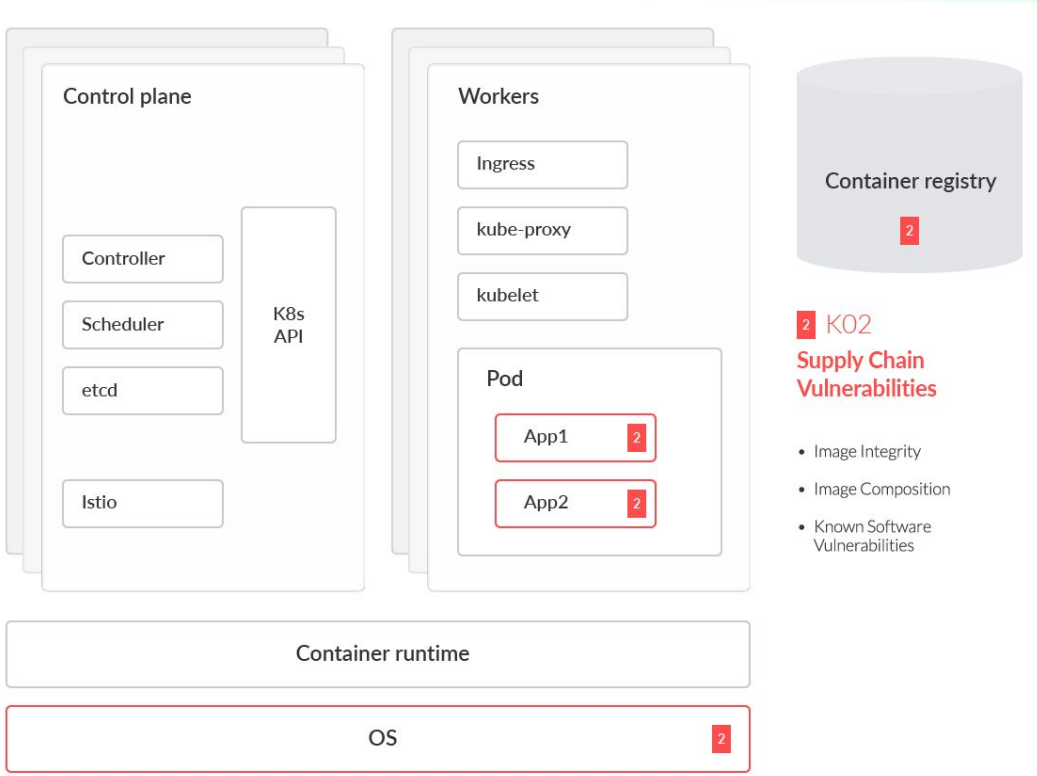
```
root@634bd4b5d3f6:/ # docker run -d -v /:/host --name escape --privileged --cap-add=ALL --pid=host --userns=host
 ubuntu sleep 3600
1696c1fd64820bfd0ce197a8bf2e3ca994cd3d44835bd0f073266d3850ab9875
root@634bd4b5d3f6:/ # docker ps
CONTAINER ID   IMAGE           COMMAND                  CREATED              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:/#
```

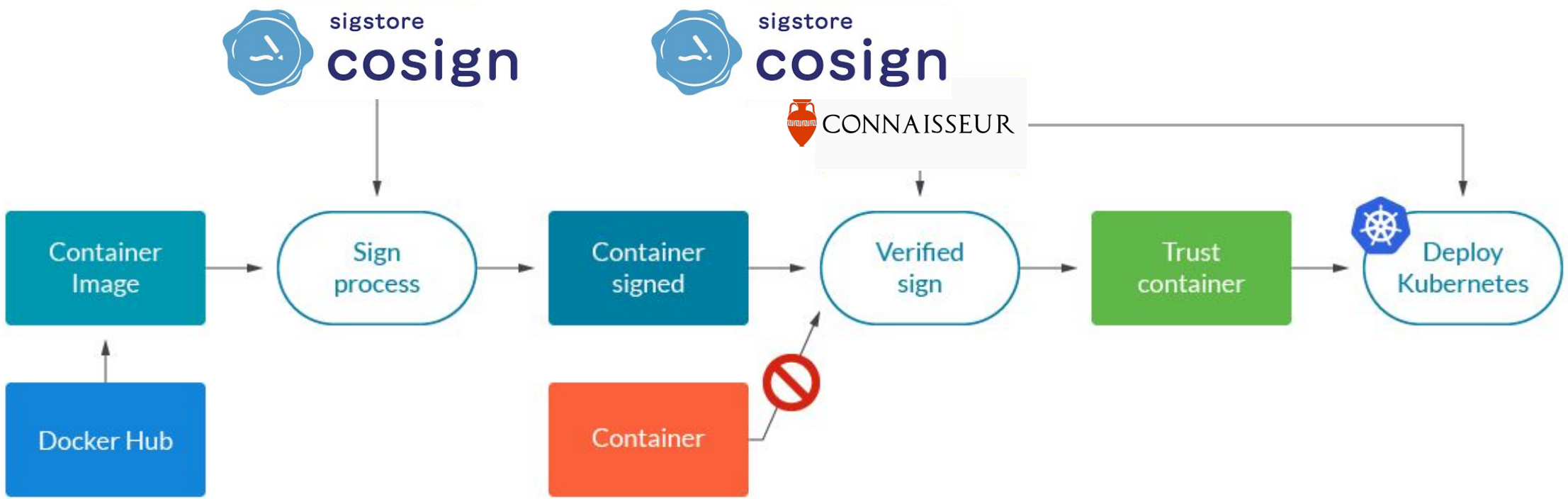
K02 - Supply Chain Vulnerabilities

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.



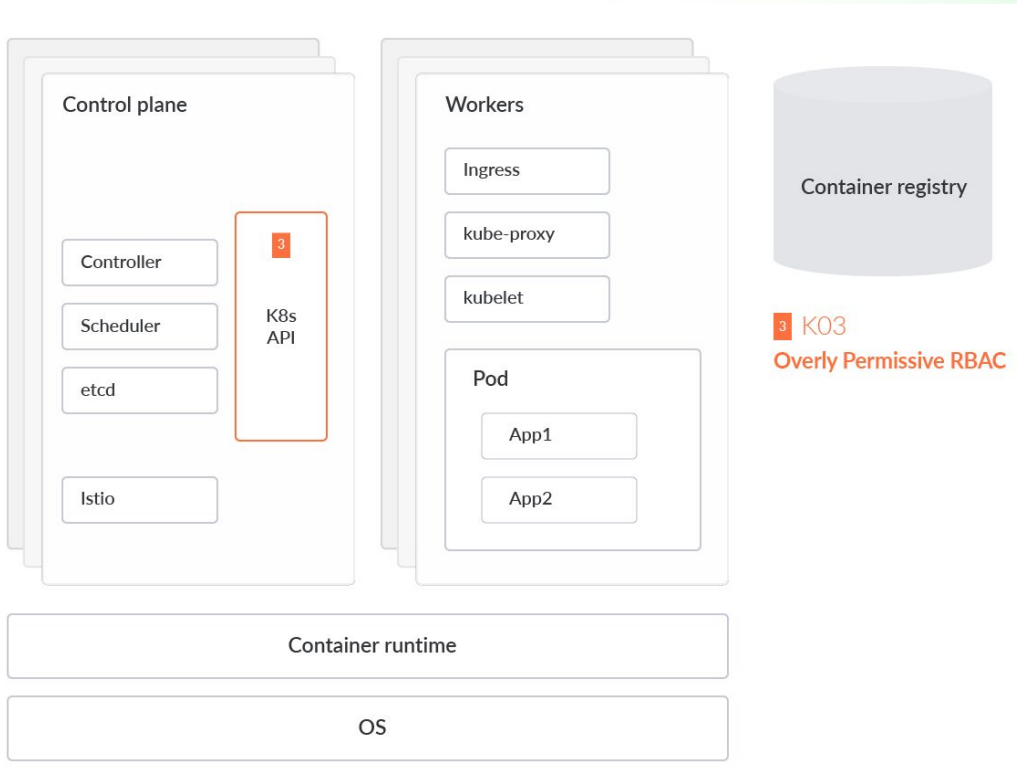

sigstore
cosign
sigstore
cosign
CONNAISSEUR
Container Image
Sign process
Container signed
Verified sign
Trust container
Deploy Kubernetes
Docker Hub
Container

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.

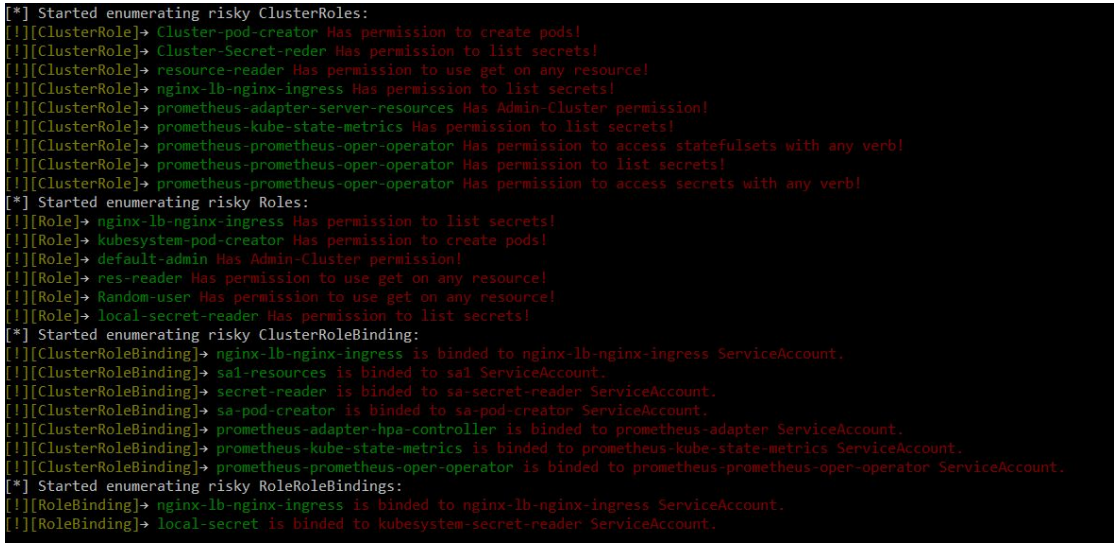


RBAC

```yaml
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/

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



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

RBAC

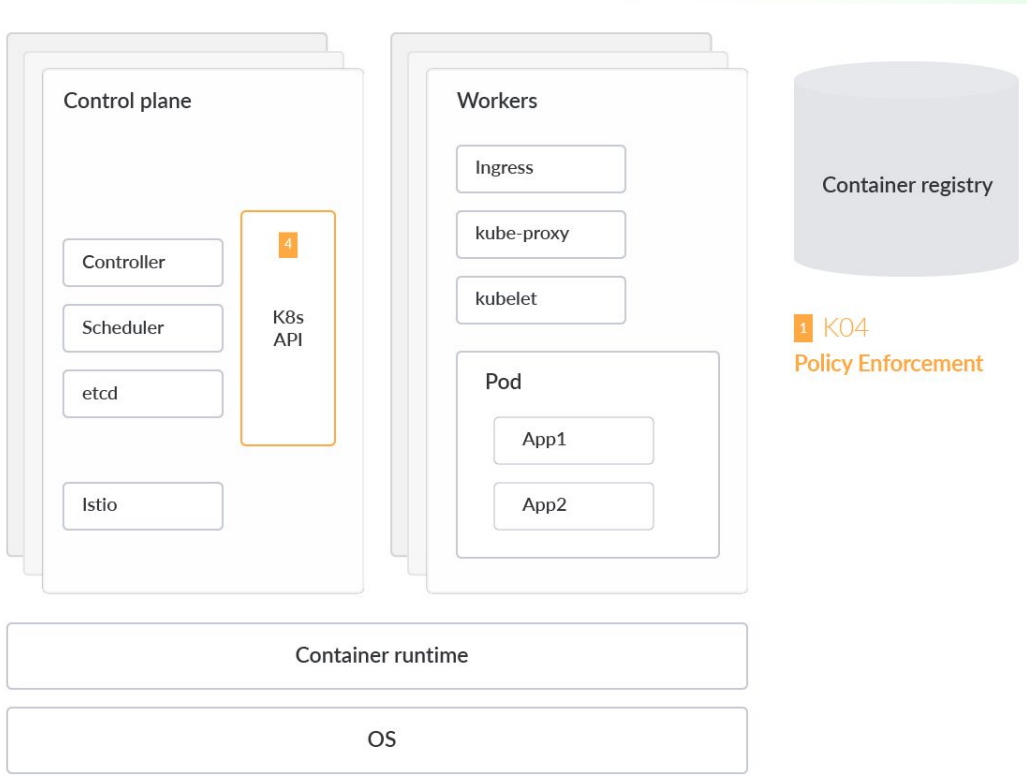
https://twitter.com/IanColdwater/status/1225949531512197126

K04 - Lack of Centralized Policy Enforcement

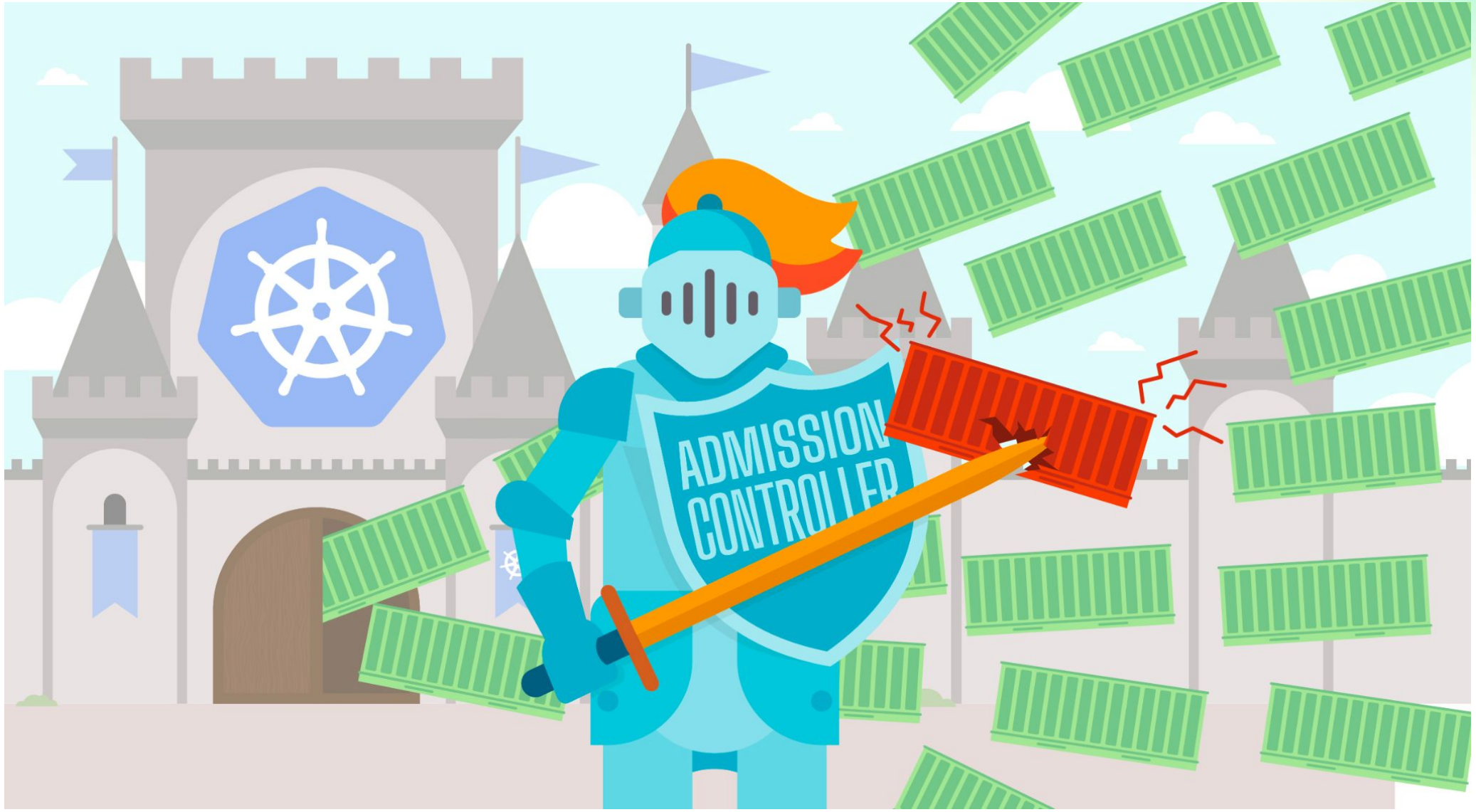
The **Admission Configuration** resource needs to be managed individually on each cluster.

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

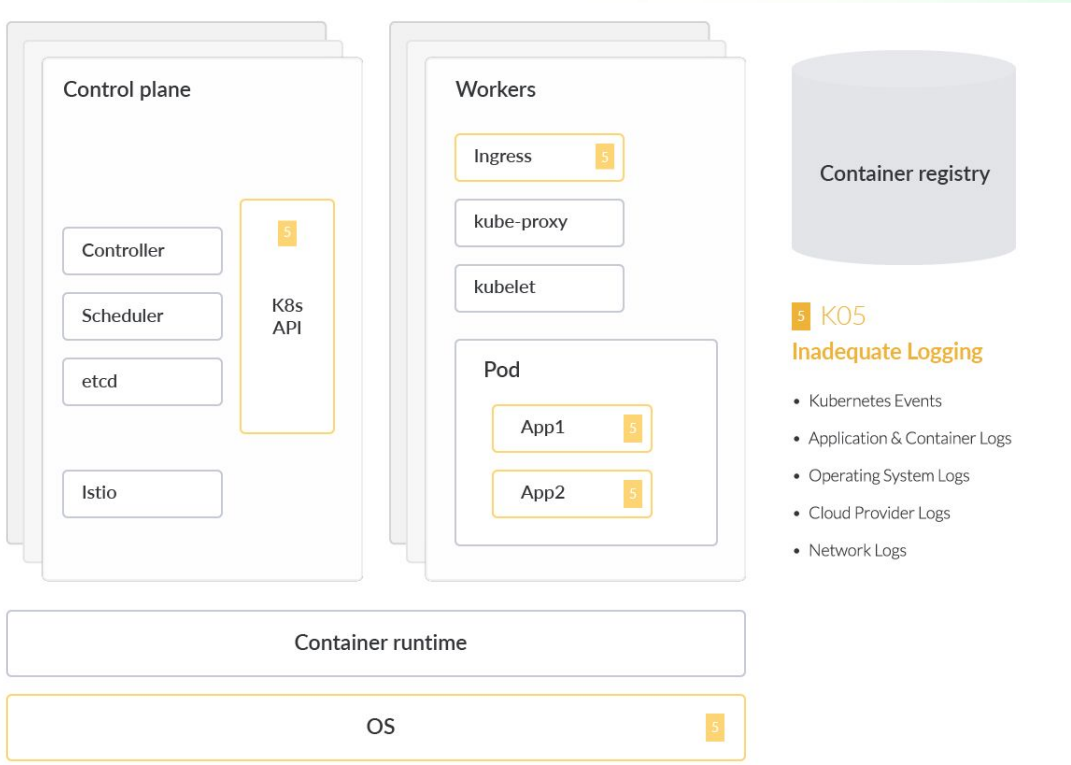


K05 - Inadequate Logging and Monitoring

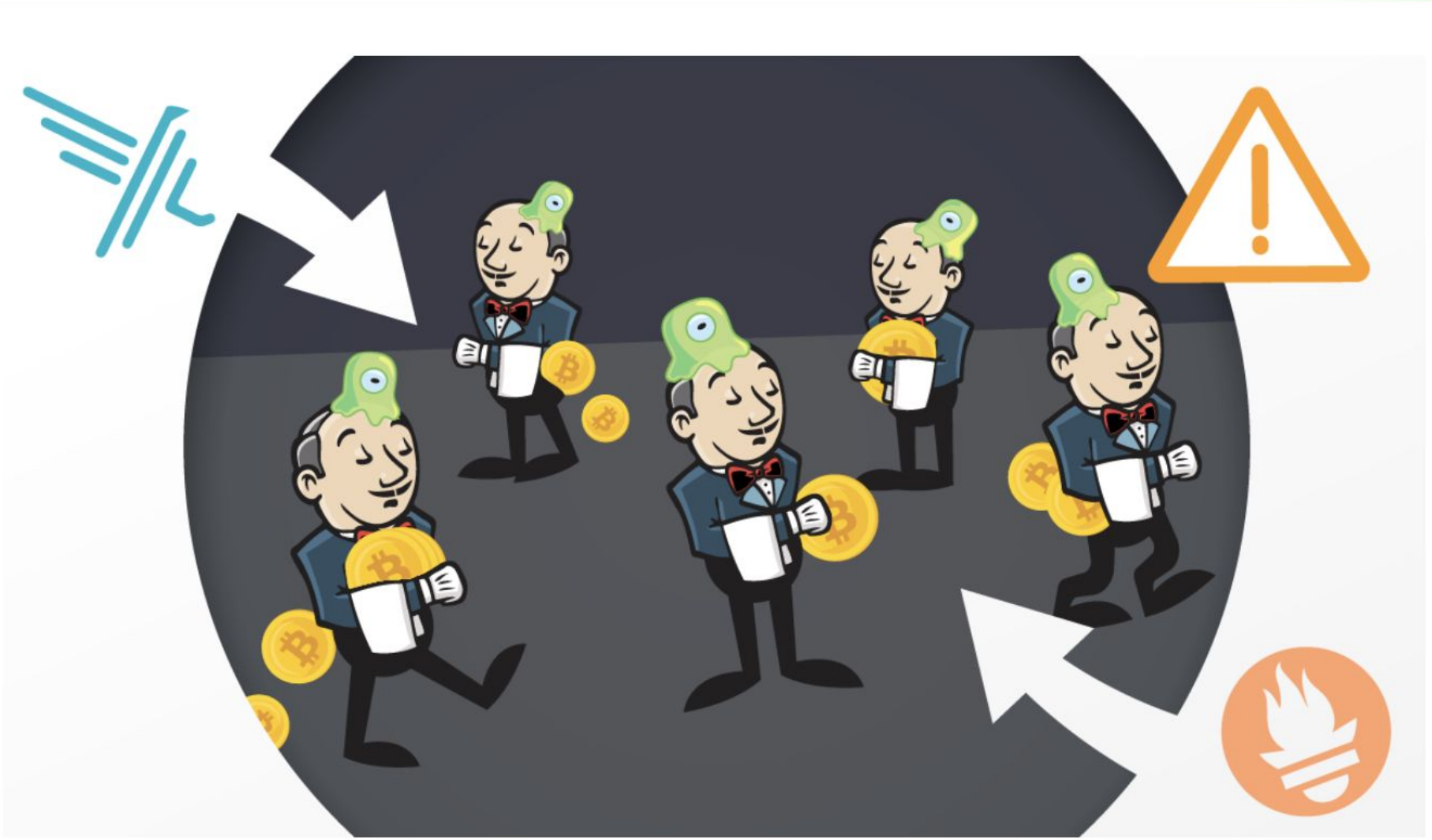
Prometheus was designed with the intention of monitoring cloud-native apps.

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



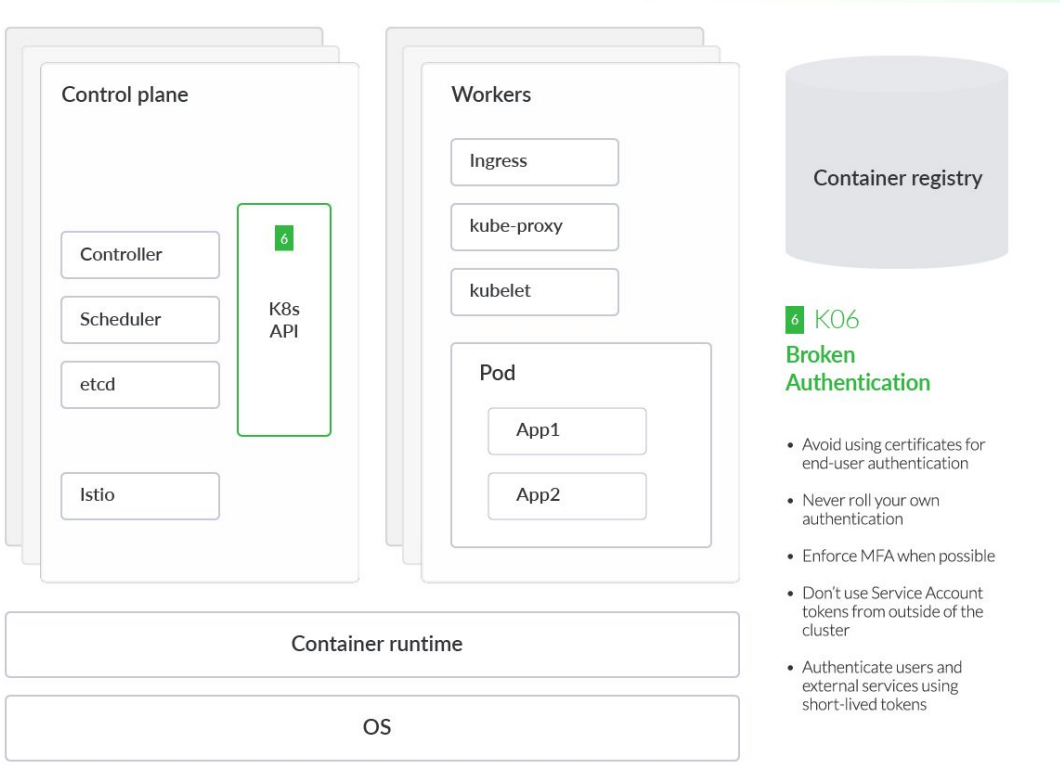
https://learn.sysdig.com/path/falco/detecting-a-crytomining-malware-attack-with-falco-and-prometheus

K06 - Broken Authentication Mechanisms

Enforce MFA where possible

Enforce RBAC Restrictions for ServiceAccounts where possible

Enforce Passwords on public-facing resources like Kubernetes dashboards

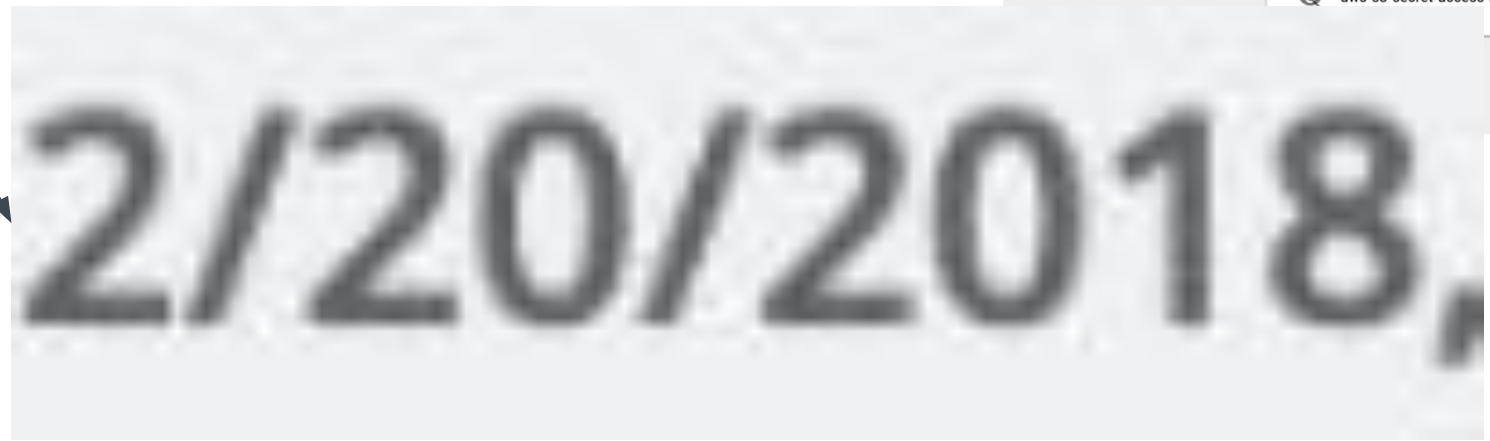


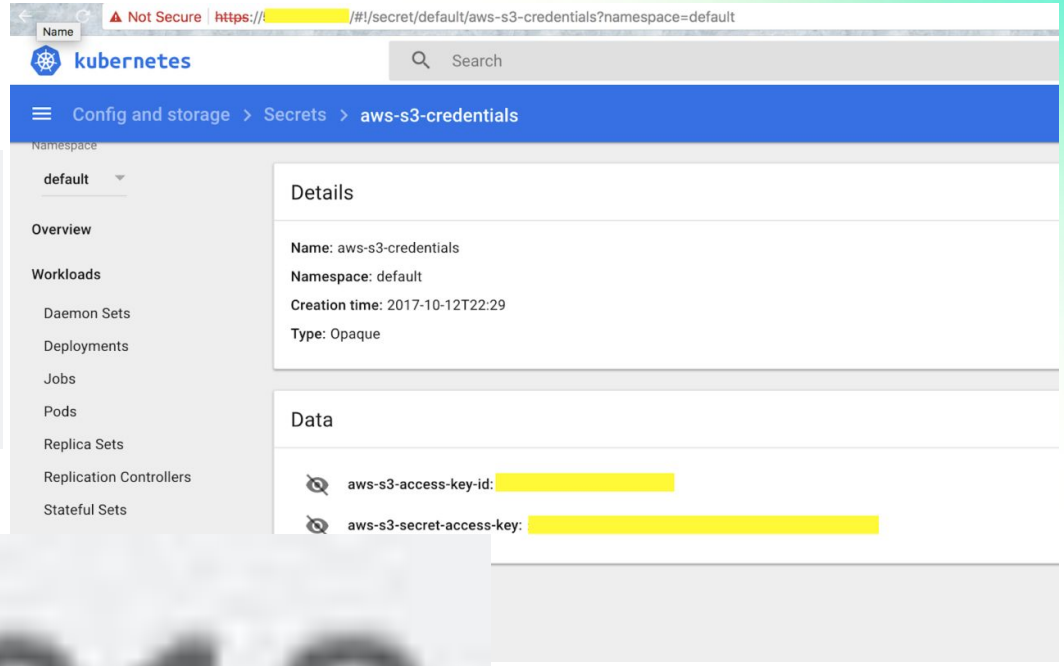
Shodan / K8s

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





Shodan / K8s

Tesla
crypt

Crooks find

DAN GOODIN - 2

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

Name

SHODAN | Explore | Downloads | Pricing | http.title:"Kubernetes Dashboard" | Account

TOTAL RESULTS

3,685

TOP COUNTRIES

United States	1,580
Canada	499
China	312
Ireland	299
India	203

More...

TOP PORTS

443	2,544
80	630
9090	226
8443	156
8000	46

More...

TOP ORGANIZATIONS

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

View Report | View on Map

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

Kubernetes Dashboard 2023-09-21T09:29:55.823549

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

SSL Certificate
Issued By:
|- Common Name: Amazon RSA 2048 M03
|- Organization: Amazon
Issued To:
|- Common Name: *.eli01.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 2023-09-21T09:22:37.416390

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:
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 2023-09-21T09:21:23.572303

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:
|- Common Name: Amazon RSA 2048 M02
|- Organization: Amazon
Issued To:
|- Common Name: *.mdaac.na3.atomx.nanostring.com
Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

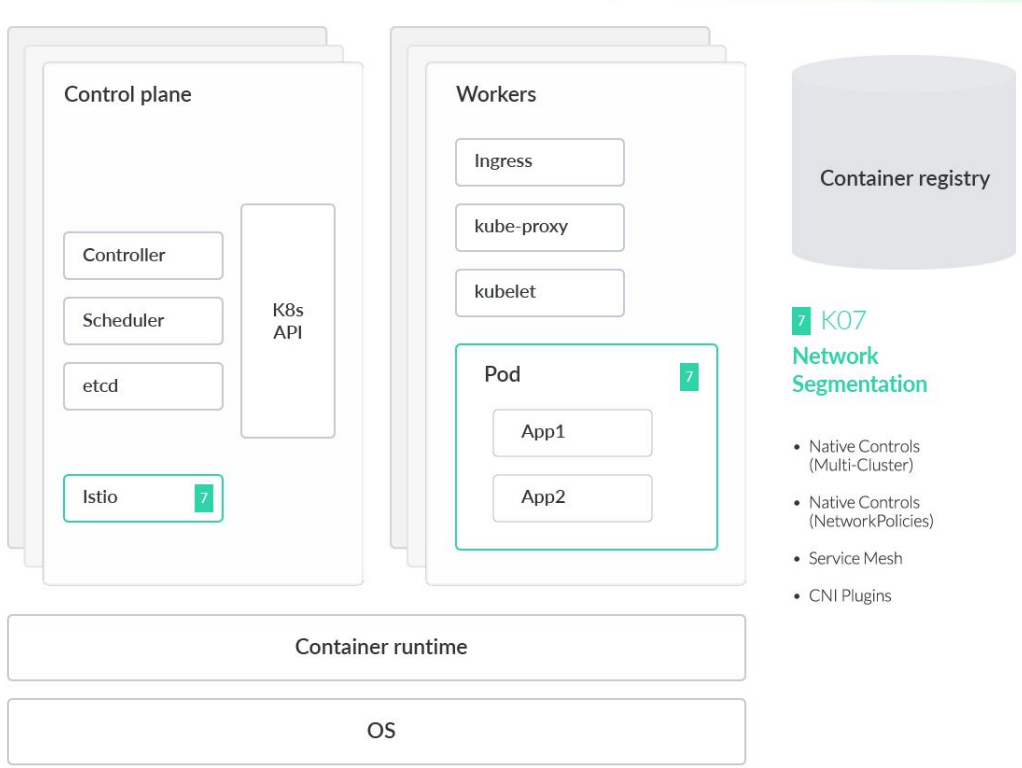
```
HTTP/1.1 200 OK
Date: Thu, 21 Sep 2023 09:21:23 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 1412
Connection: keep-alive
Accept-Ranges: bytes
Cache-Control: no-cache, no-store, must-revalidate
Last-Modified: Fri, 16 Sep 2022 11:49:34 GMT
```

K07 - Network Segmentation Controls

Istio provides a service mesh solution.

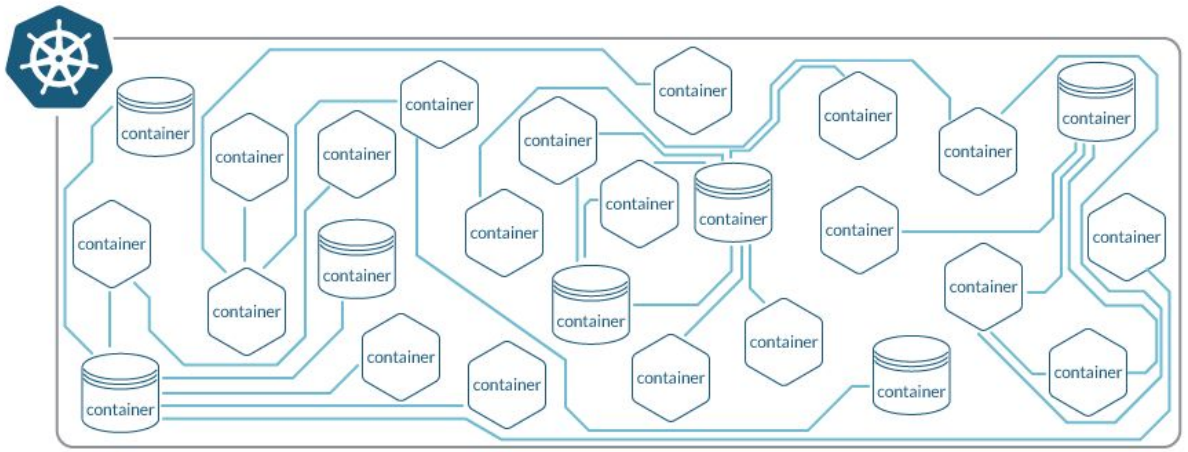
CNI like Calico & Cilium are primarily focused on L3/L4 (Network) enforcement.

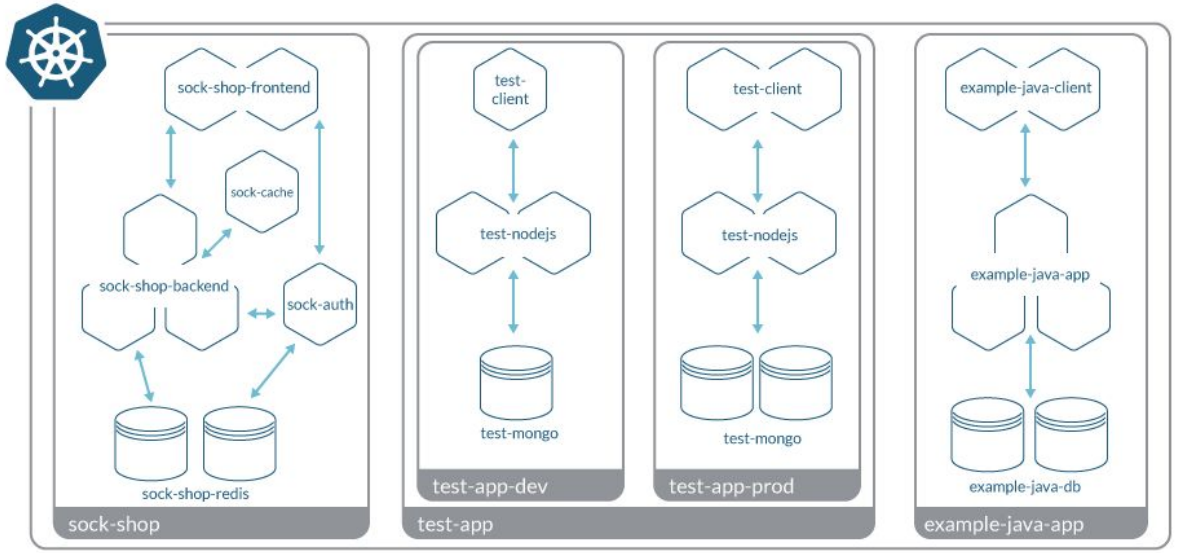
CNCF says that the majority of Kubecon participants (65%) run or plan to run between 2 and 10 Kubernetes clusters on a service mesh



Source: https://www.cncf.io/wp-content/uploads/2022/05/CNCF_Service_Mesh_MicroSurvey_Final.pdf

Service meshes, network policies deny by default, mtls with service meshes…





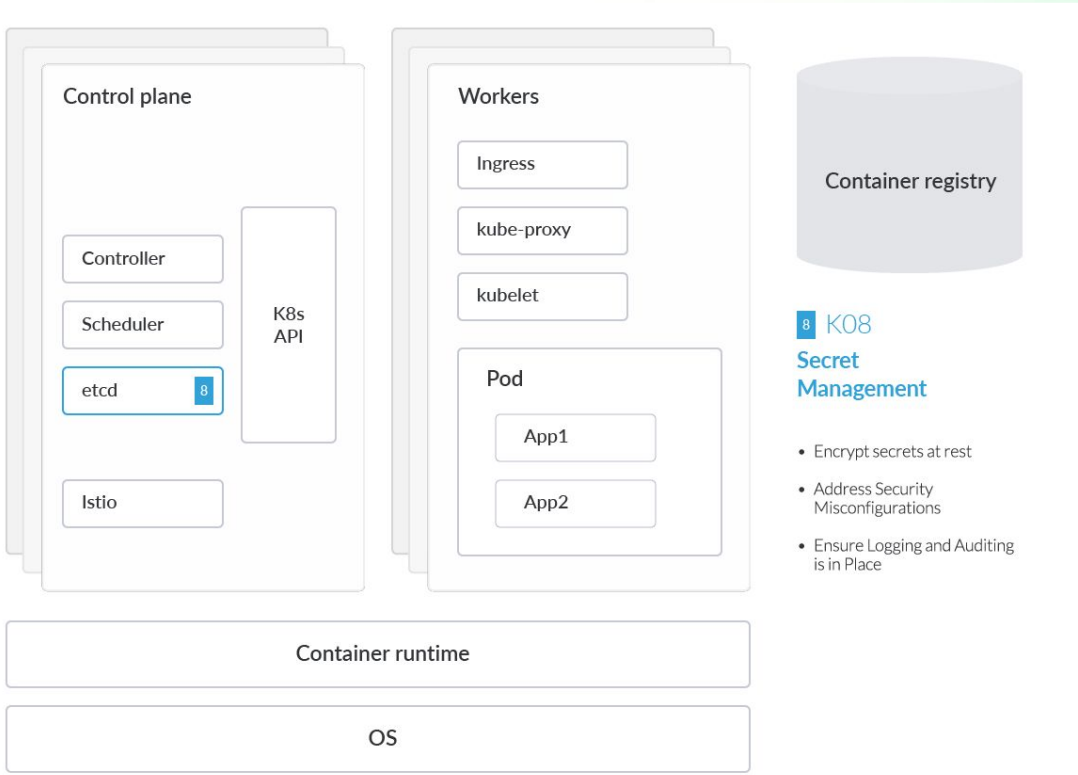
Istio

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

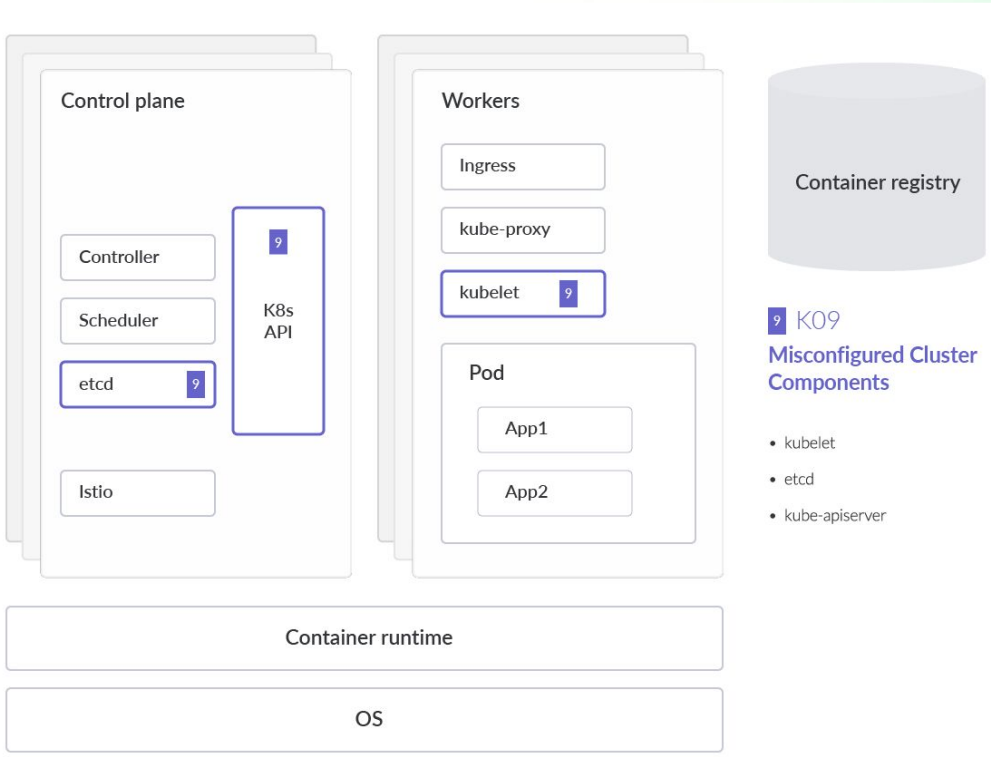
```
✖ base64-is-not-encryption master ✔ kubectl create secret generi
c demo --from-literal=password=encraption
secret "demo" created
➜ base64-is-not-encryption master ✔ kubectl exec -it -n kube-sys
tem etcd-minik
```

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.

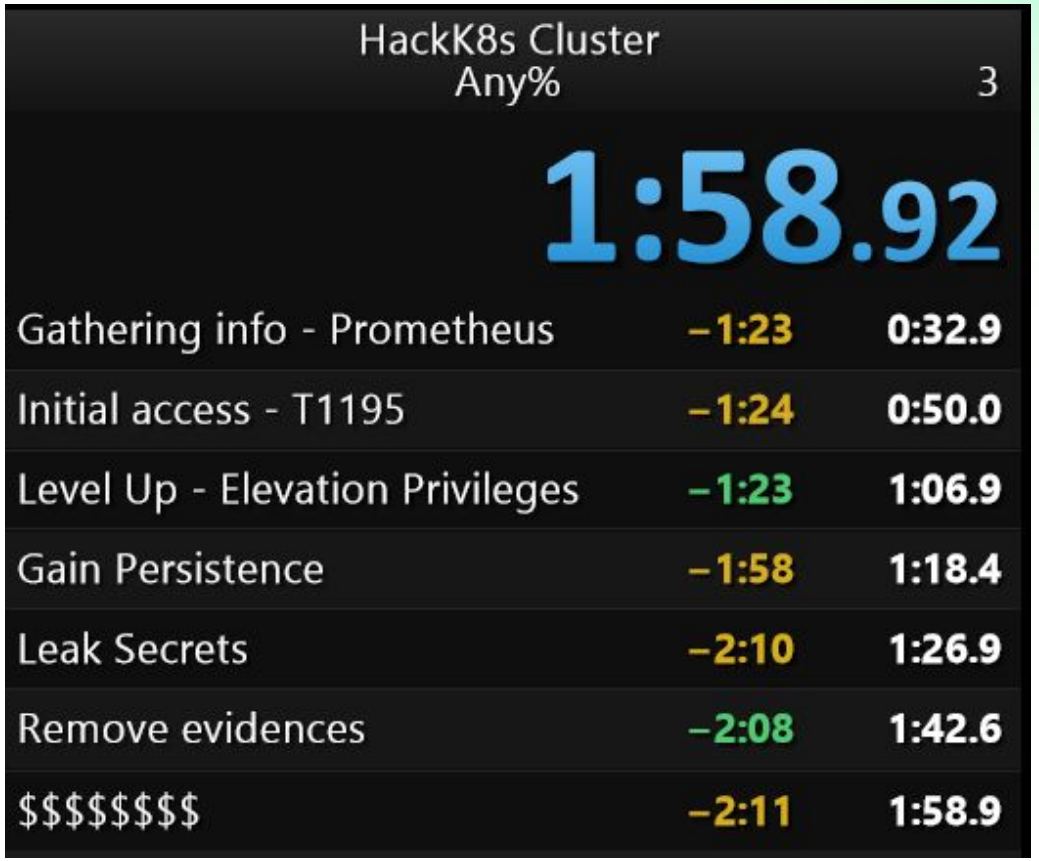


KubeCon CloudNativeCon Europe 2022

How Attackers Use Exposed Prometheus Server to Exploit Kubernetes Clusters

Miguel Hernández & David de Torres, Sysdig

https://www.youtube.com/watch?v=5cbbm_L6n7w



Cloud provider

Credentials:
- AWS Keys
- Tencent Keys
- Alibaba Keys

Networking
- Load Balancer
- Region & AZ
- VPC
- Instance IP & ID

K8s Cluster

Components:
- Kube-proxy
- Kube-admin
- Kubelet

Topology
- Cluster IP
- Namespaces
- Nodes

Known Vulnerabilities:
- CVE-2020-8554
- CVE-2020-8558
- CVE-2020-8559
- CVE-2021-25735
- CVE-2021-25737
- CVE-2021-25741

Node

- Kernel
- OS
- Go version
- Git version
- Docker

Known Vulnerabilities:
- CVE-2022-0847 - dirty pipe (Kernel Linux)
- CVE-2022-0185
- USN-3833-1: Linux kernel (AWS) vulnerabilities
  - CVE-2018-18955
- CVE-2021-3156

Pod / Container

Registry:
- docker.io

Image:
- Image-id

Service
- Service-example
  - Website
  - API
  - …
  - https://example.com

Known Vulnerabilities:
- CVE-2021-44521 - Cassandra
- https://mariadb.com/kb/en/security/ - RCE
- CVE-2020-28035
- Wordpress
- CVE-2018-16850 - PostgreSQL
- CVE-2019-11043 - PHP
- CVE-2021-44228 - Log4j
- CVE-2022-22963 - Spring Cloud
- CVE-2020-13942 - Apache unomi

Kubernetes Secrets

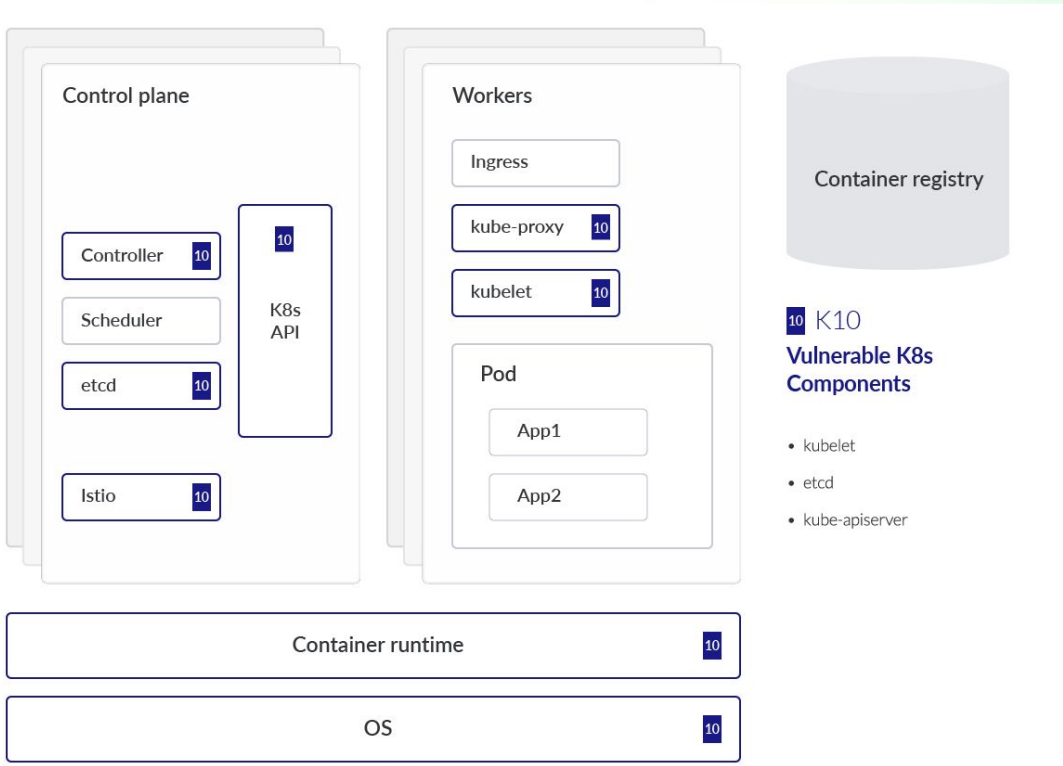
- Service auth tokens

K10 - Outdated & Vulnerable K8s Components

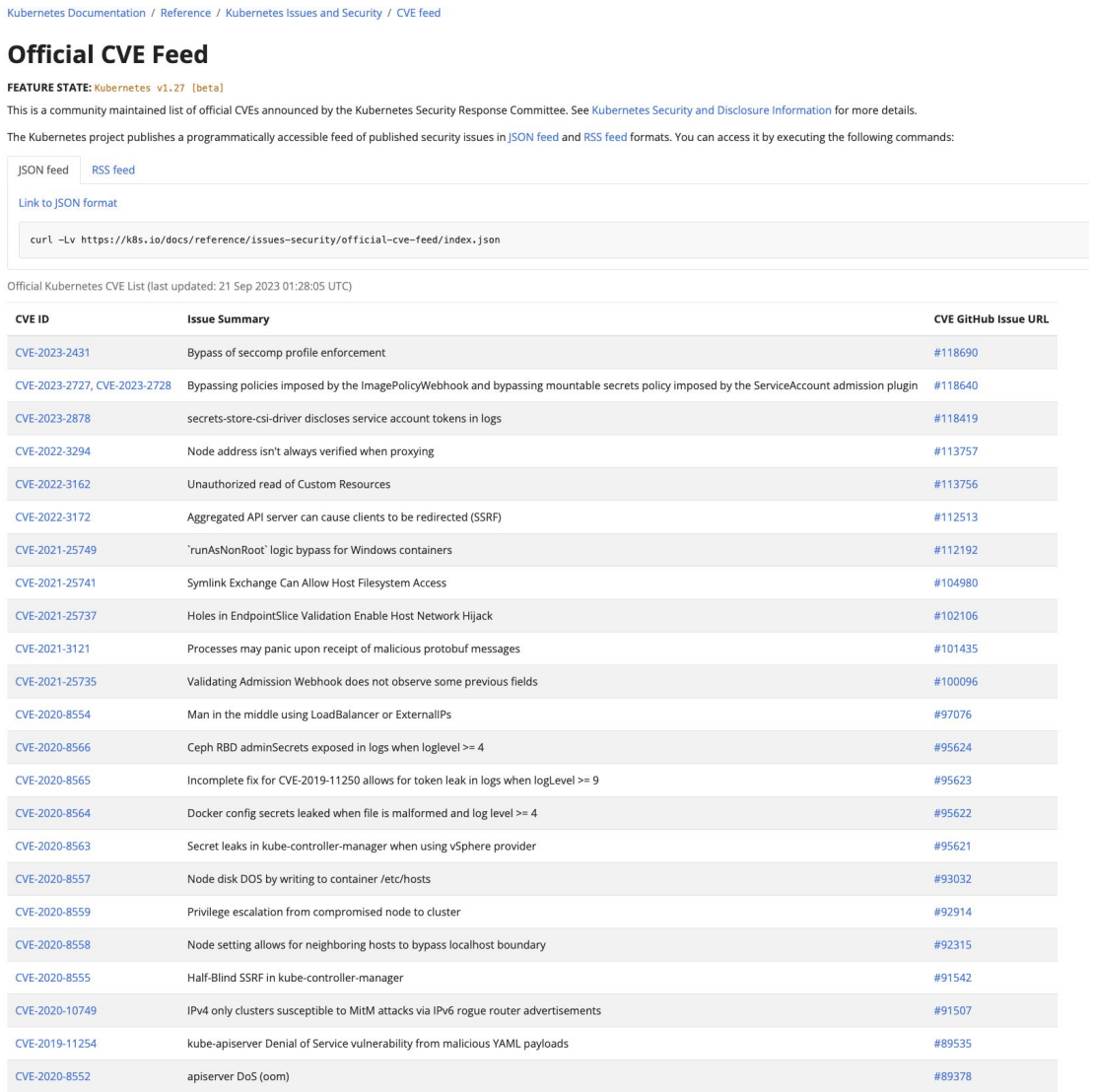
CVE-2018-18264 – Privilege escalation through Kubernetes dashboard

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

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.

Q & A

Thank you!