alcide

Kubernetes Security Anatomy

& the recent CVEs perspective

Gadi Naor, CTO

Alcide

Jul 2020

AlciderbaK AlcidesKan AlcideAdvisor AlcideRuntime AlcidekAudit

In today’s session

- Kubernetes Security Building Blocks
- Demos
- The Recent Kubernetes CVEs (CVE-2020-10749 & CVE-2020-8555)
- Detection & Preventions

Yours Truly

about# gadi.naor

--from tel_aviv

--enjoy sk8boarding

--kernel-dev @check_point --kernel-dev @altor_networks --kernel-dev @juniper_networks

--cloud-native @alcideio

validate k8s cluster

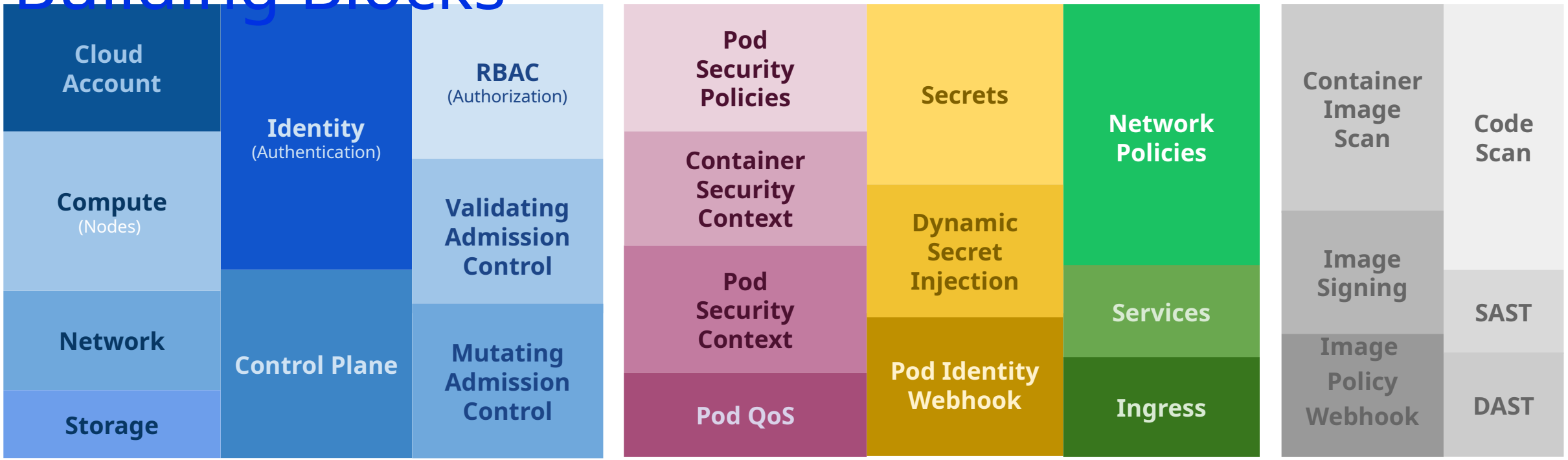
AlcidesKan

AlcideAdvisor

AlcideRuntime

AlcidekAudit

Kubernetes Security Building Blocks



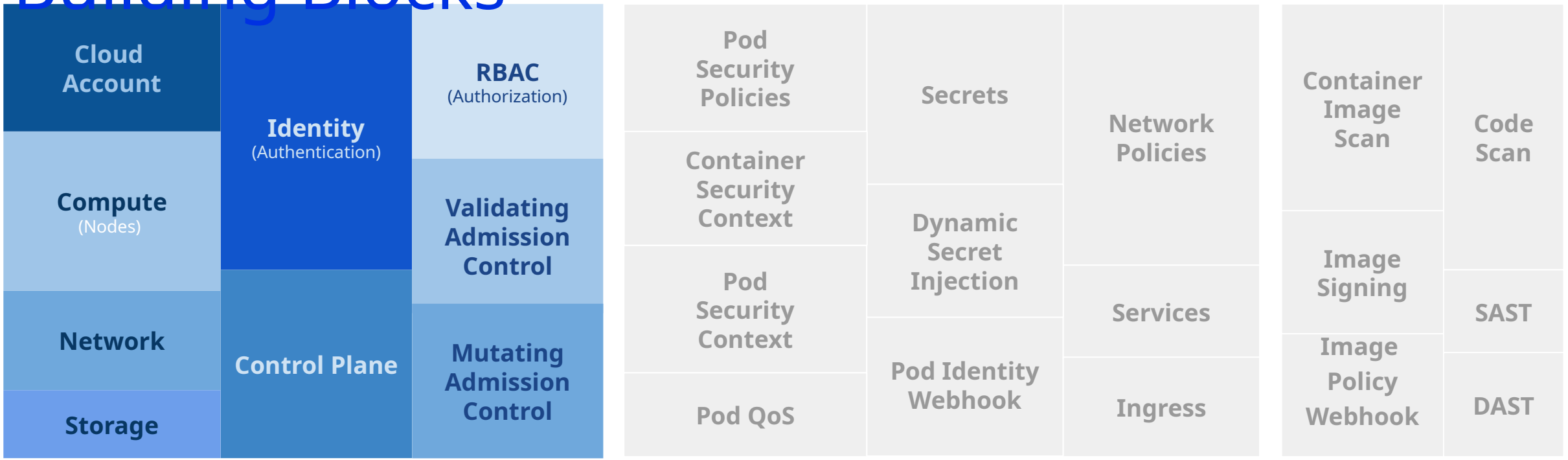
Cloud + Cluster

Workloads

App Code

~~Kubernetes~~ Security Building Blocks

Kubernetes Security Building Blocks

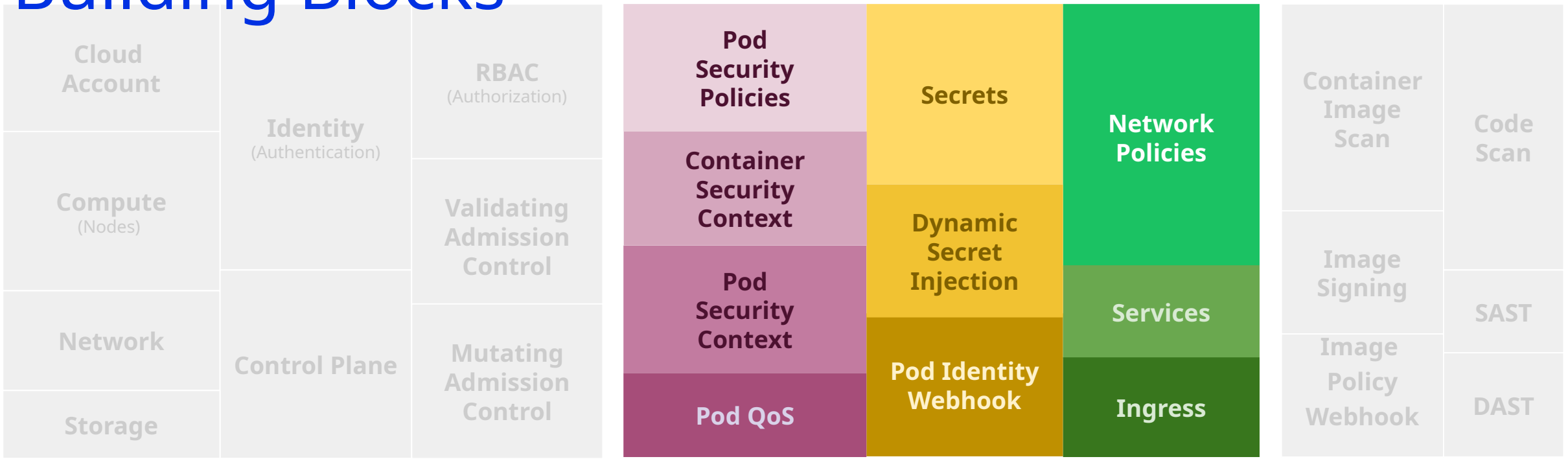


Cloud + Cluster

Workloads

App Code

Kubernetes Security Building Blocks

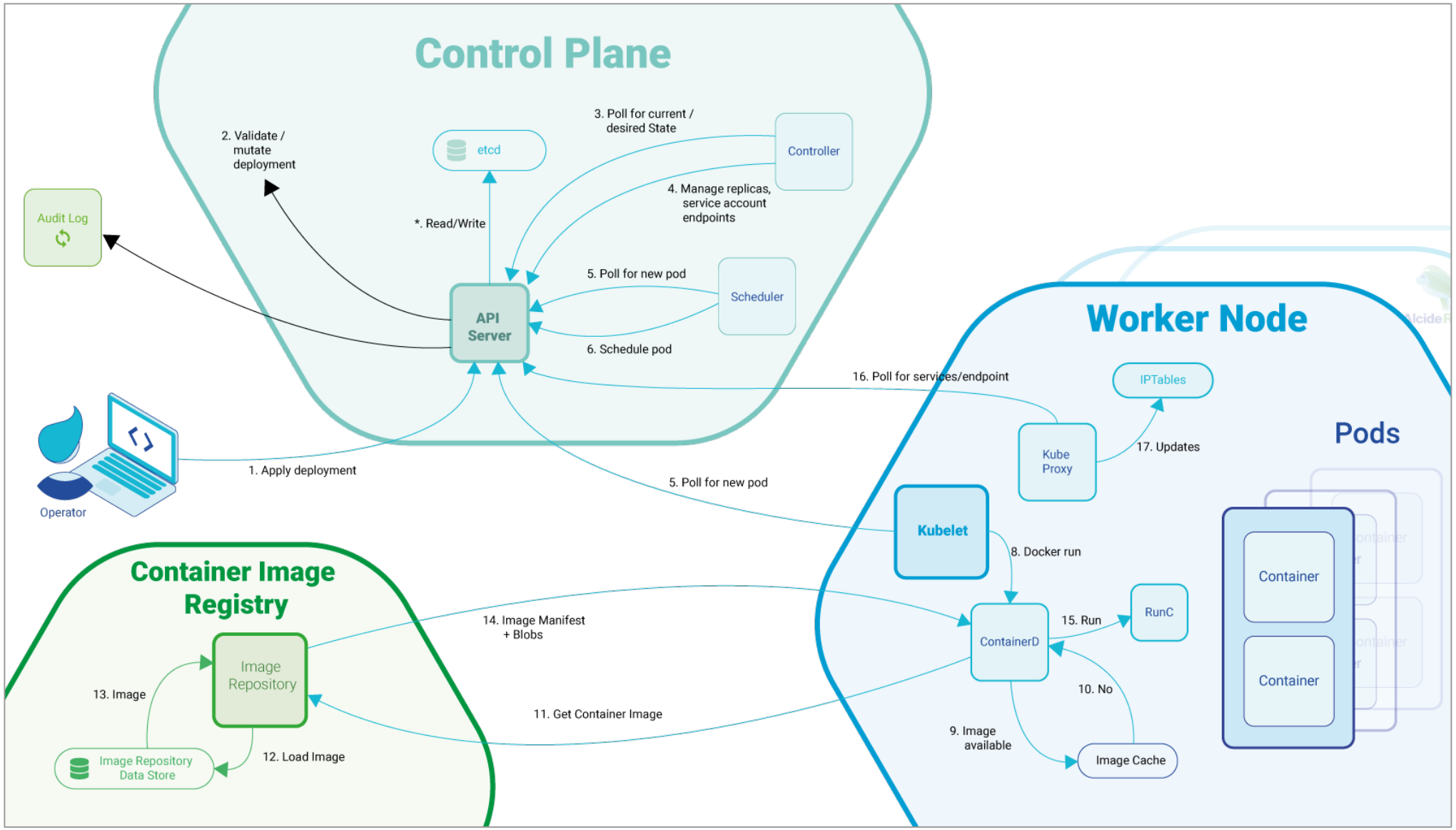


Cloud + Cluster

Workloads

App Code

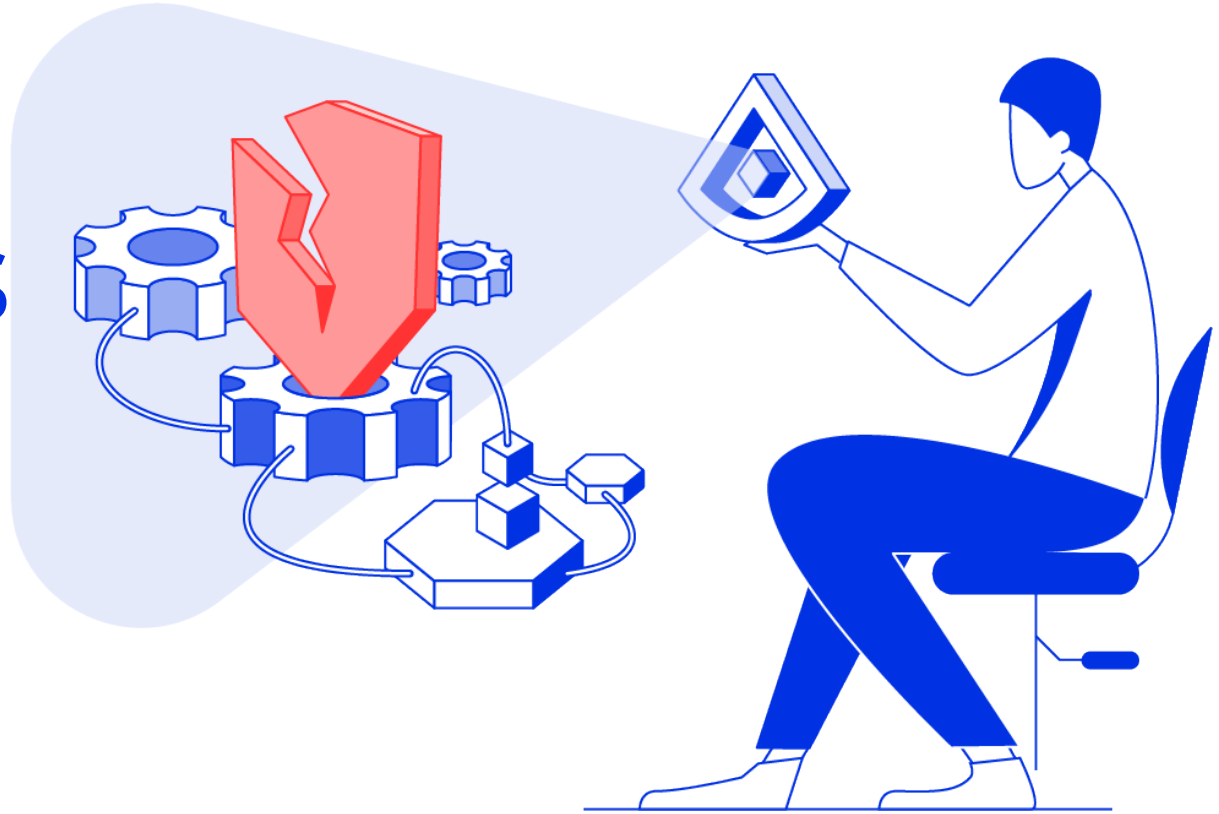
Trust Boundaries



Know Thyself & Know Thy Cluster(s)

1) **Exception Management** - how do you manage for the various building blocks those exceptions?
   - Examples: Exclude namespaces, Exclusion within namespace, Exclusion based on label selector
2) **Multi Cluster**- how do you unify the application of security blocks?
   - Examples: PCI regulated applications, Stage + Prod, Multiple Applications
3) **Multi Cloud** - unifying security is very challenging
   - Examples: Kubernetes Audit Log, Pod Identity, Cloud Account ...
4) **Security Life Cycle** - Life span longer/different than cluster lifespan
   - Examples: Secrets (API Keys, Token,..), User Identity, Certificates, ...
5) **"Shift Left"** - Integrate Security Tools to your pipelines (CI + CD)

Scan Your Clusters



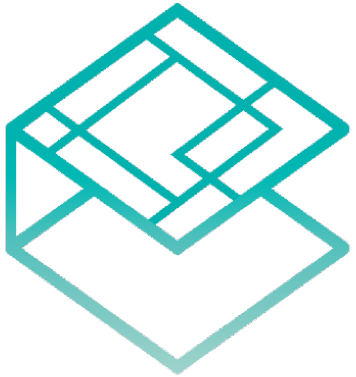
CVEs & Kubernetes

- CVE ⇒ Common Vulnerabilities and Exposures
- Kubernetes (and Golang) - not immune to bugs nor security bugs
- K8S has a vulnerability disclosure process
- Bug Bounty program if you feel like hacking for living is your thing
- 2 Most recent CVEs: **CVE-2020-8555 & CVE-2020-10749**

CVE-2020-10749

Man-In-The-Middle (MiTM) Attack Leverages IPv6 Router Advertisements

- ❑ Not core k8s vulnerability
- ❑ Forwarding Plane/CNI specific weakness
- ❑ **CAP_NET_RAW** - Sending ICMPv6 messages is a prerequisite for this exploit
- ❑ Istio is not useful at helping this type of attack vectors
- ❑ Think zero-trust // if something is not explicitly allowed → it's denied/blocked



CVE-2020-10749

Man-In-The-Middle (MiTM) Attack Leverages IPv6 Router Advertisements

Mitigate:
→ Deny/Block IPv6 malicious traffic
→ ….Do not run (network) privileged containers
→ ….Disable OS Kernel features

Fix:
→ Upgrade vulnerable CNI

CVE-2020-8555

Half-Blind Server-Side Request Forgery (SSRF) in kube/cloud-controller-manager

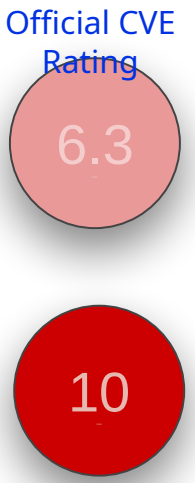
```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: slow
provisioner: kubernetes.io/glusterfs
parameters:
  resturl: "http://127.0.0.1:8081"
  clusterid: "630372ccdc720a92c681fb928f27b53f"
  restauthenabled: "true"
  restuser: "admin"
  secretNamespace: "default"
  secretName: "heketi-secret"
  gidMin: "40000"
  gidMax: "50000"
  volumetype: "replicate:3"
```

Official CVE Rating

Self Rated @ Managed K8S

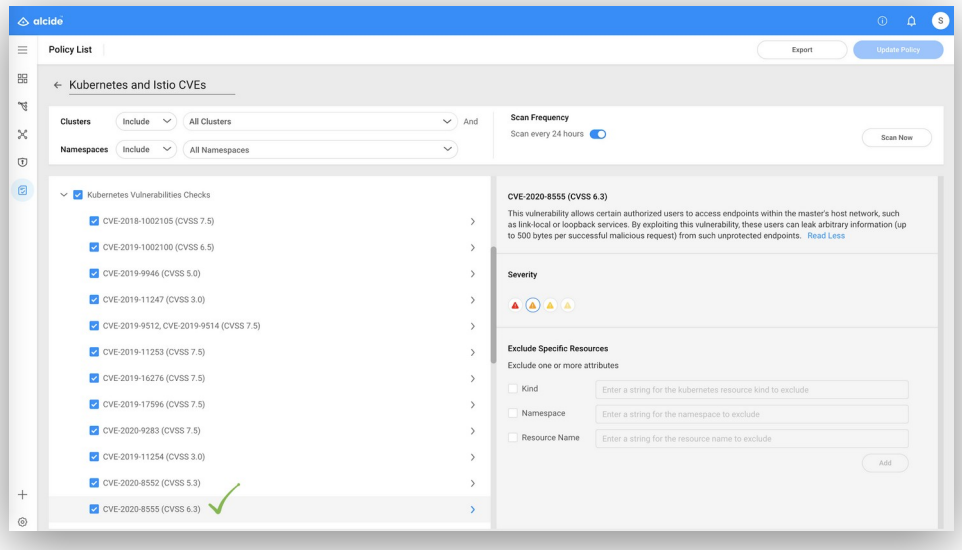
CVE-2020-8555 // Disclosure Timeline

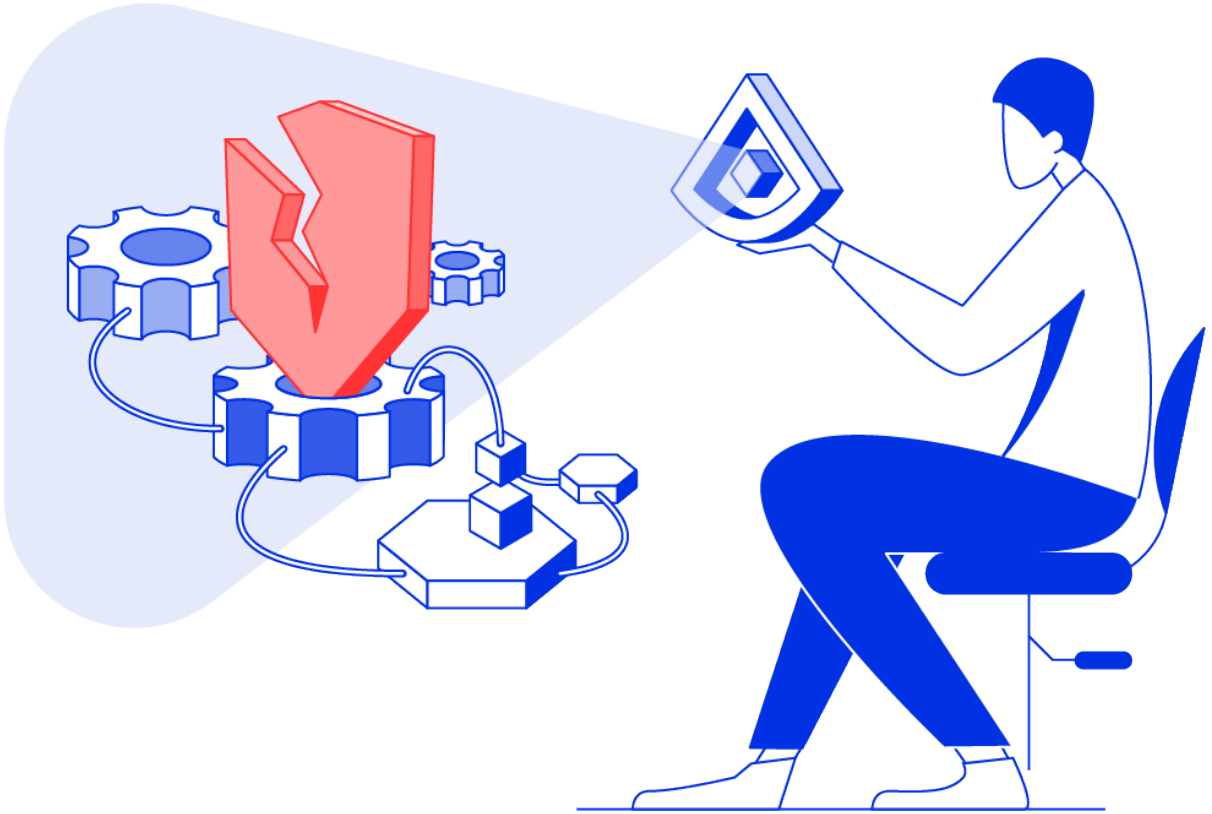
- ➔ **6th December 2019** : MSRC Bug Bounty case submission
- ➔ **3rd January 2020** : K8s has been informed by a third-party actor about the security issue discovered.
- ➔ **15th January 2020** : K8s team provided with technical and generic report k8s HackerOne bug bounty program.
- ➔ **15th January 2020** : Kubernetes noticed us that the half blind SSRF part + CRLF injection for old releases was being considered as an in-core vulnerability.
- ➔ **15th January 2020** : Bounty Received from MSRC through HackerOne
- ➔ **16th January 2020** : Kubernetes PSC (Product Security Committee) acknowledged the vulnerability and requested us the **mid-march embargo** due to the numerous distributors involved on this security matter.
- ➔ **11th February 2020** : Bounty received from Google VRP
- ➔ **4th March 2020** : Bounty received from Kubernetes through HackerOne
- ➔ **15th March 2020** : Initial planned public disclosure delayed due to COVID-19 situation
- ➔ **1st June 2020** : Kubernetes + Microsoft Public Disclosure
  - ❑ v1.0-1.14
  - ❑ versions prior to v1.15.12, v1.16.9, v1.17.5,
  - ❑ v1.18.0



alcide

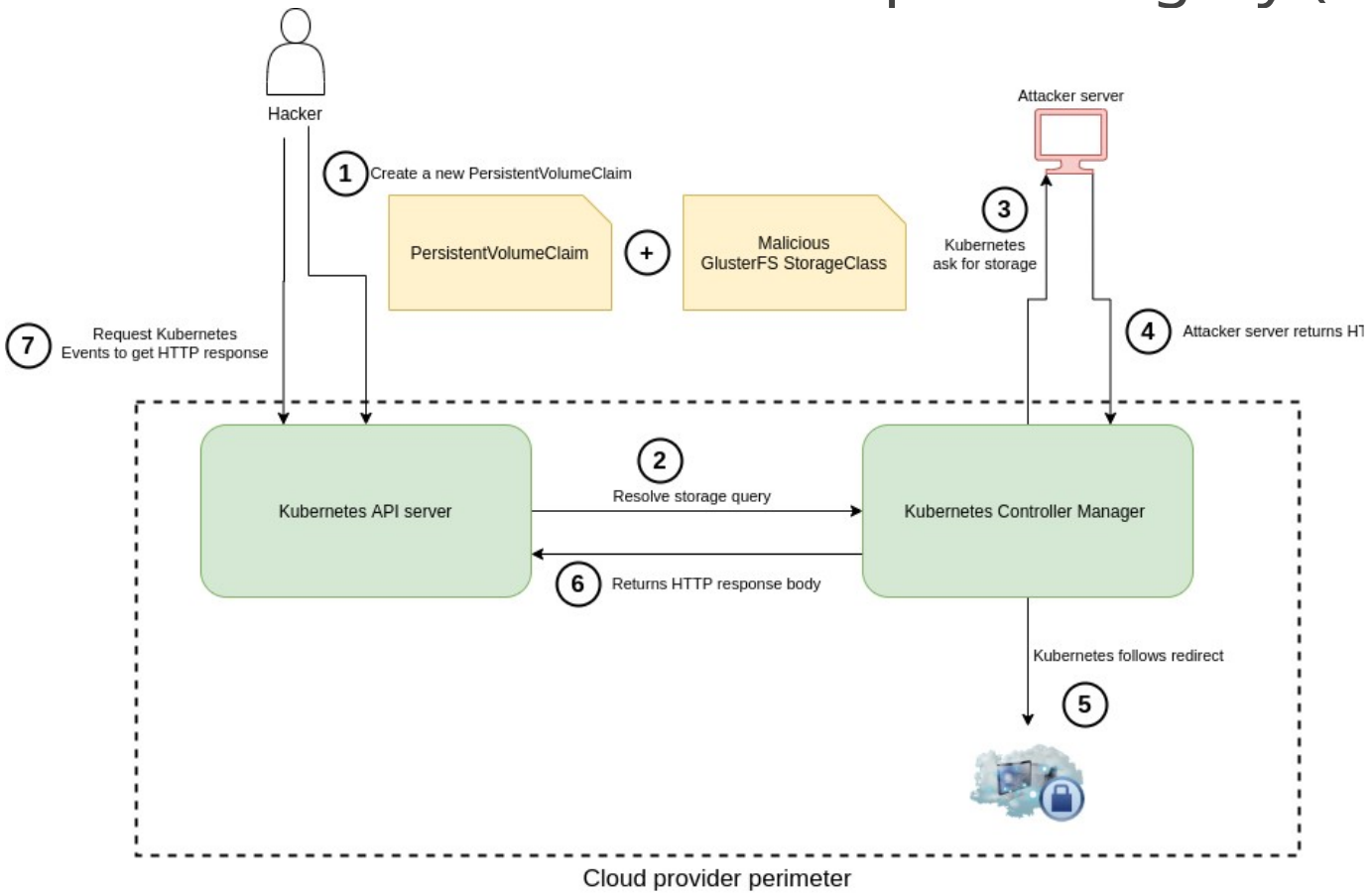
Scan Your Clusters





CVE-2020-8555

Half-Blind Server-Side Request Forgery (SSRF) in kube/cloud-



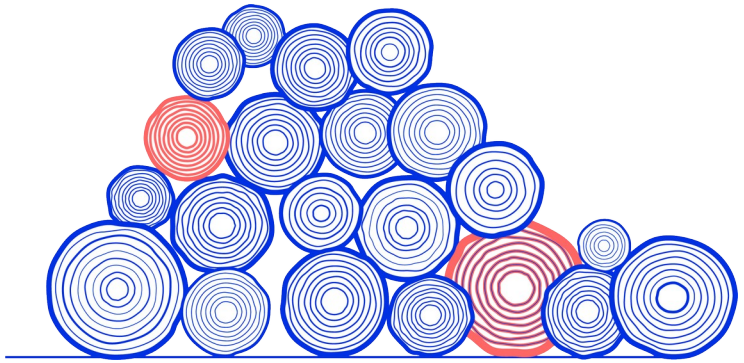
1) **Create** Malicious **StorageClass** + **Create PVC**
2) **kube-apiserver** resolve storage query
3) **kube/cloud-controller-manager** ask for storage
4) attacker reply with HTTP redirect (302)
5) **kube/cloud-controller-manager** follows redirect
6) **kube/cloud-controller-manager** return HTTP response
7) **kubectl get events** to read HTTP response

 source: https://medium.com/@BreizhZeroDayHunters/when-its-not-only-about-a-kubernetes-cve-8f6b448eafa8

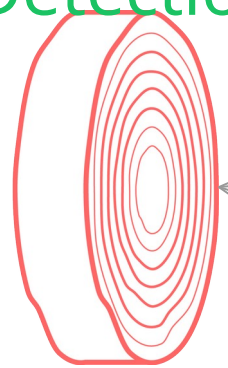
Kubernetes Audit Logs - Security Gold Mine

Detect threats using Kubernetes Audit logs

Raw Audit Logs



Analysis & Detection



- Exploited vulnerabilities in Kubernetes API server
- Stolen credentials
- Stolen tokens
- Compliance based policies
- Misconfigured RBAC

Security Issues that Kubernetes Customers Face

Users, Activities, Exposure

Stolen Credentials

The Result: Gaining initial access to cluster

Stolen Token

The result: Performing lateral movement, privilege escalation, data access and data manipulation while evading detection

Misconfigured RBAC

The result: Performing lateral movement, privilege escalation, data access and data manipulation while evading detection

Exploited Vulnerabilities in Kubernetes API Server

The result: Gaining access to privileged and sensitive resources

alcide

Try Alcide Kubernetes Security

- Security Scan Your Cluster - Alcide Advisor (Free)

  alcide.io/pricing/free-forever

- Kubernetes Security Monitoring - Alcide kAudit a

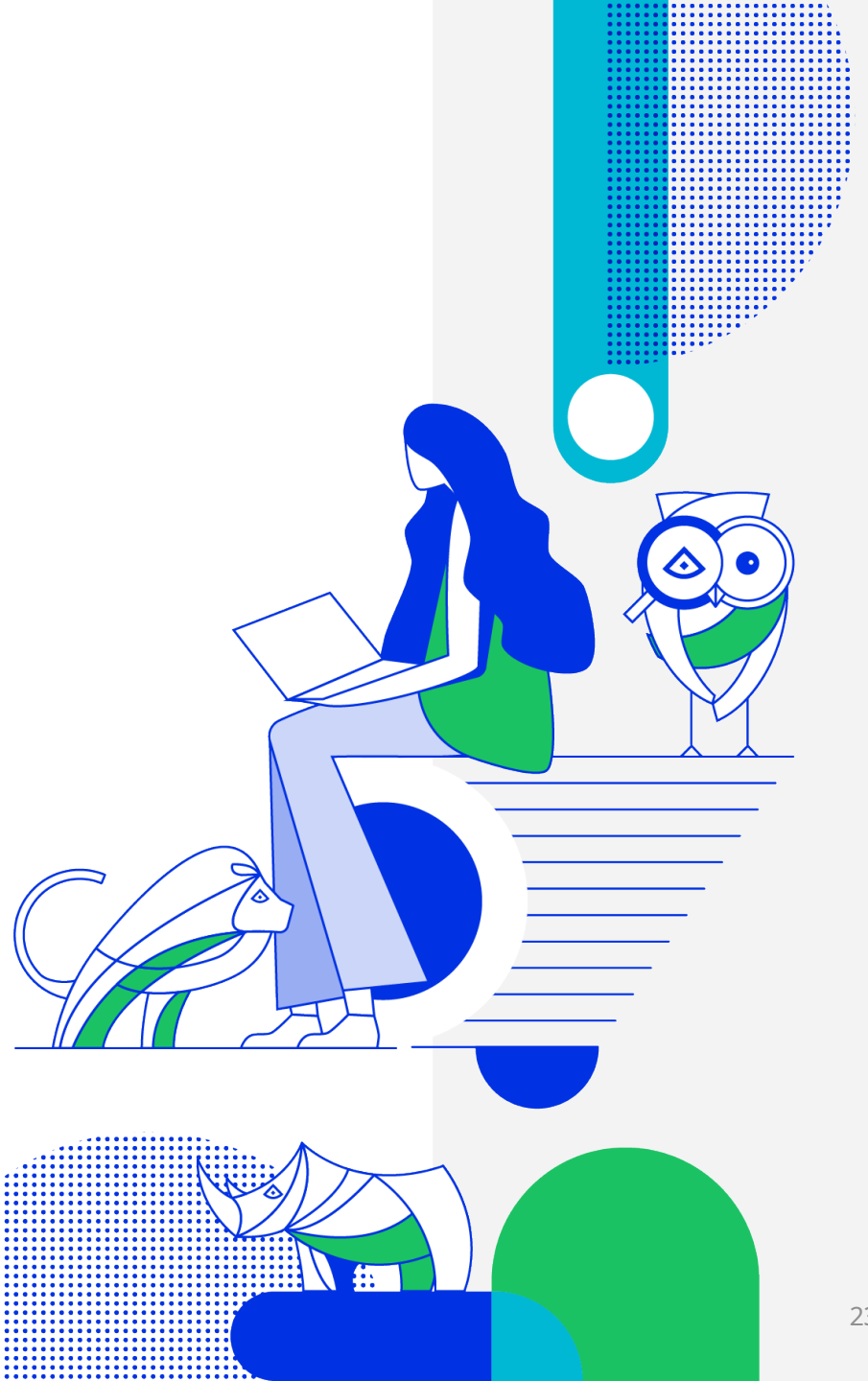
  lcide.io/kaudit-K8s-forensics

- Open Tools

  github.com/alcideio

- Tutorials

  codelab.alcide.io



THANK YOU!

www.alcide

@alcideio
@gadinaor