ALL YOUR CONTAINERS ARE BELONG TO US

James Condon
BSidesSF19
March 4th, 2019

AGENDA

- whoami
- Kubernetes overview
- Dashboard
- API Server
- etcd
- Final thoughts

whoami

- James Condon, Director of Research @ Lacework
- Former USAF OSI, Mandiant, and ProtectWise
- Network Forensics, Incident Response, Threat Intelligence, Cloud Security

@laceworklabs

@jameswcondon

- Networking
- Provisioning
- Storage
- Redundancy
- Auto-Scaling
- Security

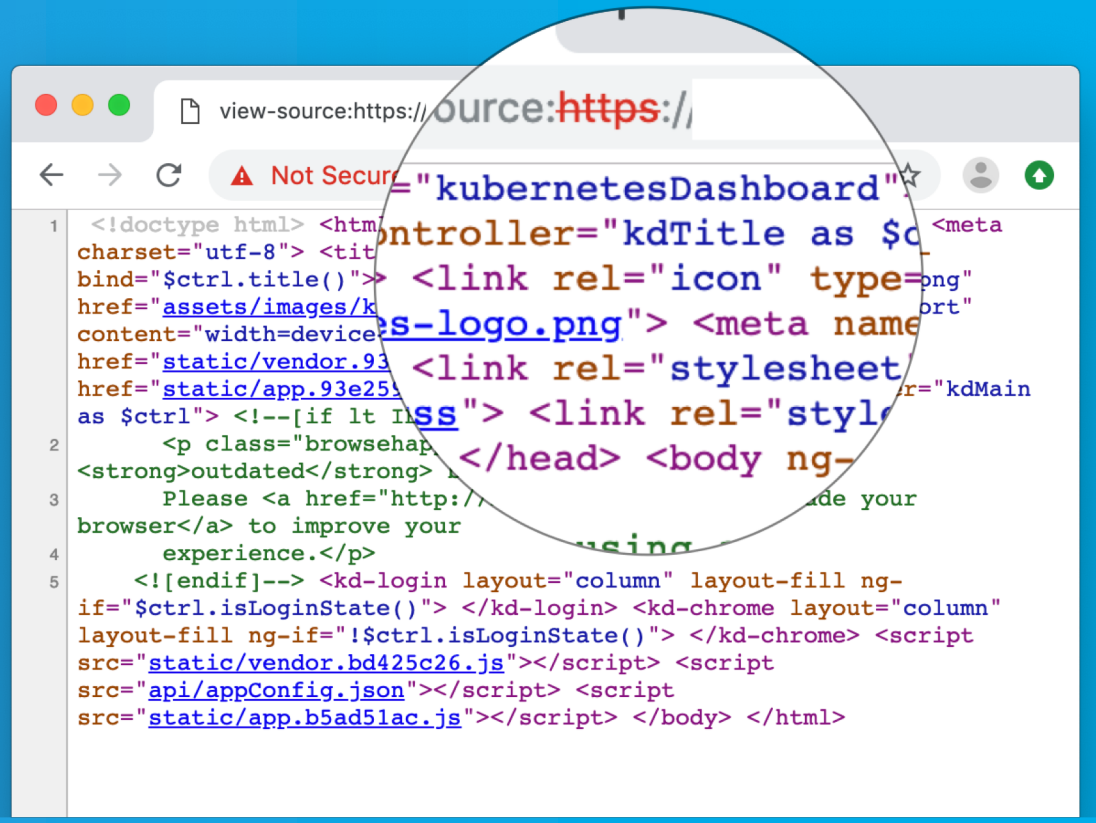

THAT KUBERNETES, SO HOT RIGHT NOW
memegenerator.net

RESEARCH DISCLAIMERS

- No containers were harmed in the making of this presentation
- Promote awareness & enhance security
- Recommendations for managing your own cluster

KUBERNETES DASHBOARD

- Cluster management UI
- Web based
- Default service account needs RBAC
- Dashboards in the news ⬇



AVIVA™

TESLA

gemalto
security to be free

WeightWatchers

censys

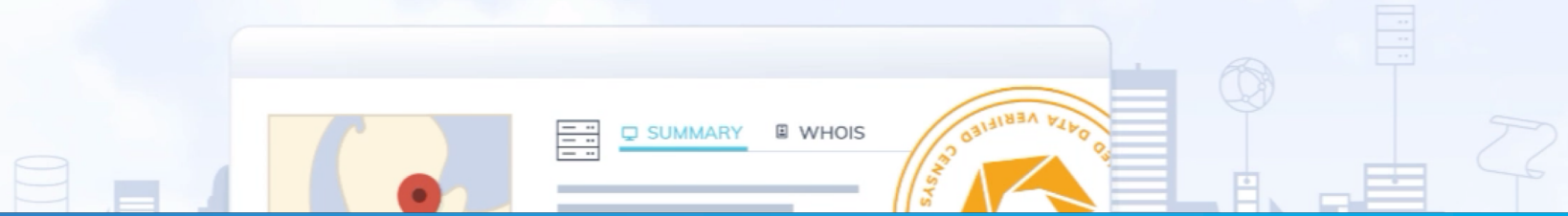
HOW WE HELP PRICING ABOUT LOGIN

Security starts with visibility

Find and monitor every server on the Internet

What servers and devices are exposed on my network?

Enter an IP address or CIDR block (141.211.0.0/16)



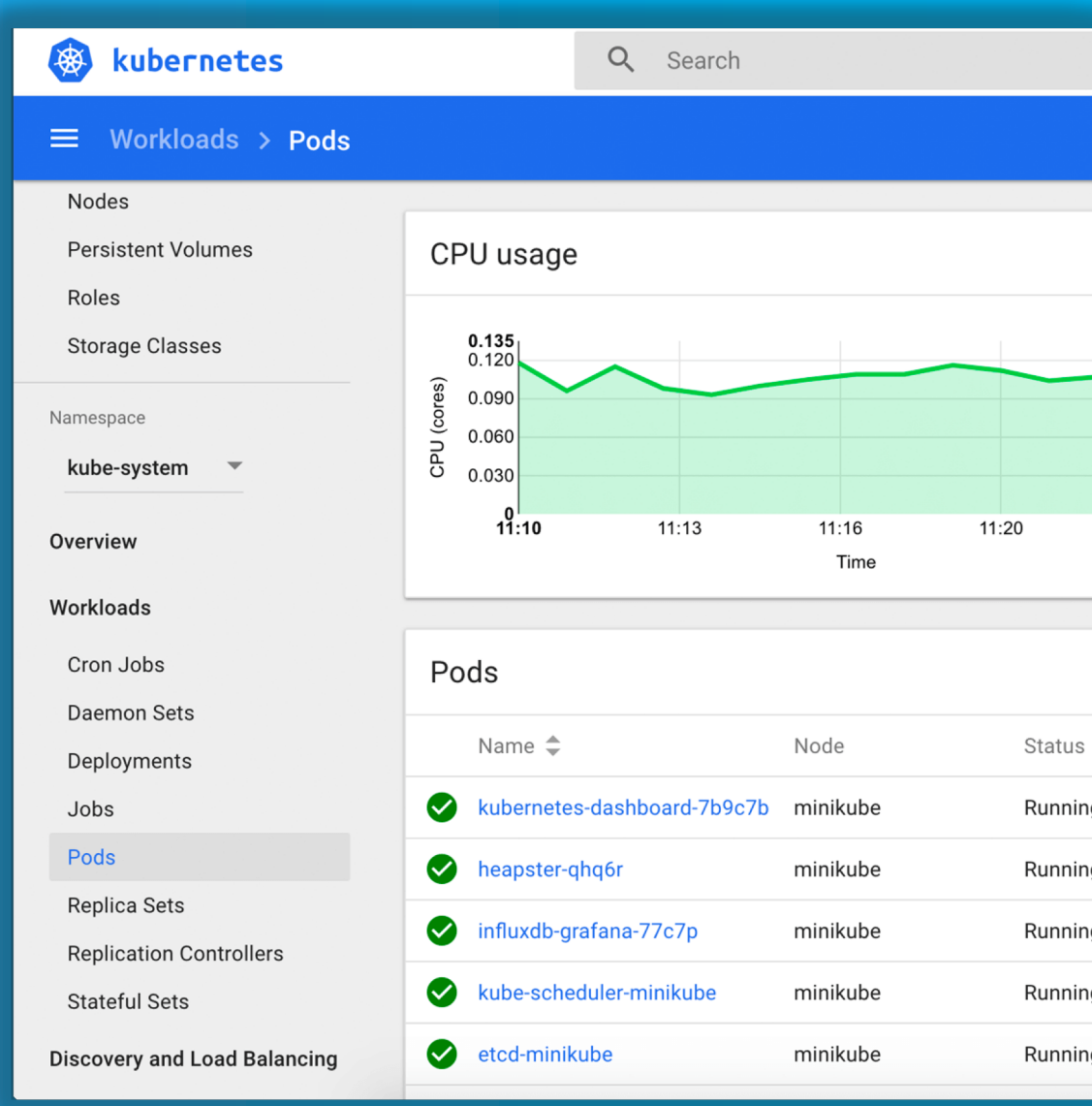
DASHBOARD FINDINGS

500+

- 75% AWS
- 10% GCP + Azure
- Ports 80, 443, 8080

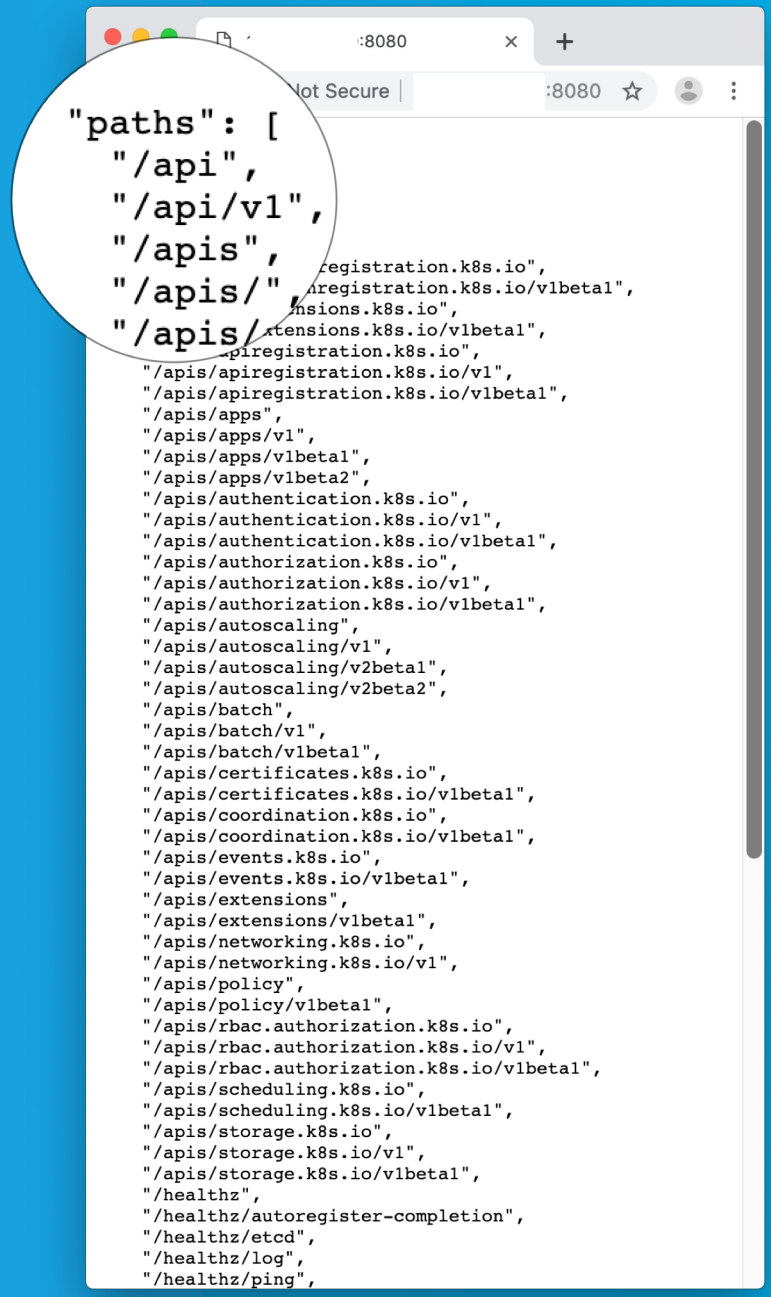
DASHBOARD RECOMMENDATIONS

- Disable (if possible)
- Ensure RBAC is enabled
- Don’t elevate privileges on default service account
- Avoid internet access, otherwise use VPN, Bastion, etc



KUBERNETES API SERVER

- Fundamental component of Kubernetes
- REST API
- Handles authentication and authorization
- Secure & **insecure port** by default
- CVE-2018-1002105



censys

HOW WE HELP ▾ PRICING ABOUT LOGIN

Security starts with visibility

Find and monitor every server on the Internet

What servers and devices are exposed on my network?

Enter an IP address or CIDR block (141.211.0.0/16)

Elements Console Sources Network Performance

View: Group by frame Preserve log Disable ca

Filter Hide data URLs

All XHR JS CSS Img Media Font Doc WS Manifest Other

50 ms 100 ms 150 ms 200 ms 250 ms

Name	Sta...	Type	Initiator	Size	Time	Waterfall
censys.io	200	do...	Other	13....	72 ...	

API SERVER FINDINGS

21K+

- 92% AWS, ~3% GCP + Azure
- ’18: 21K+ for K8s, Meso, OpenShift, & Swarm
- Cert CNs: kubernetes-master 88%, system:apiserver 4%, apiserver 2%

API SERVER FINDINGS (INSECURE PORT)

800+

API SERVER RECOMMENDATIONS

- Restrict network access
- Disable insecure port
- Enable RBAC
- Look into advanced authentication options
- Upgrade

ETCD

- Distributed key value datastore
- Maintains cluster state and secrets
- No authentication by default
- No encryption at rest by default
- REST & gRPC APIs
- The Luke Hemsworth of unsecured DBs

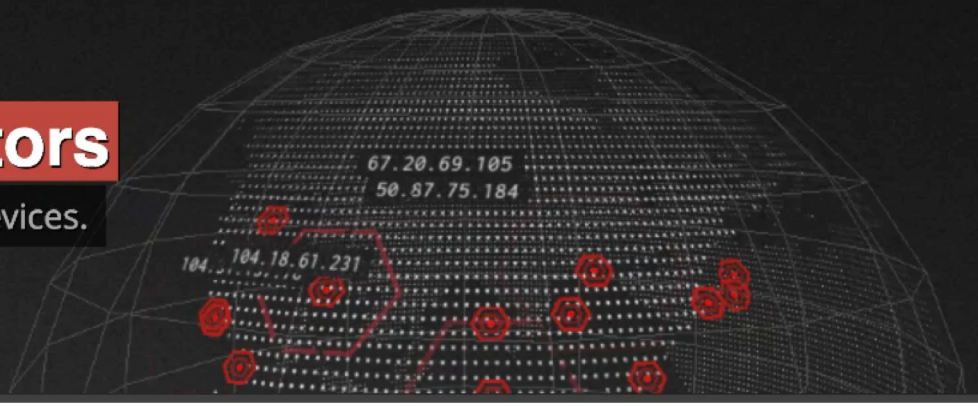
Shodan | Developers | Book | View All... | Show API Key | Help Center

SHODAN | Explore | Downloads | Reports | Developer Pricing | Enterprise Access | My Account

The search engine for Refrigerators

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account | Getting Started



Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

56% of Fortune 100

1,000+ Universities

Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.

Analyze the Internet in Seconds

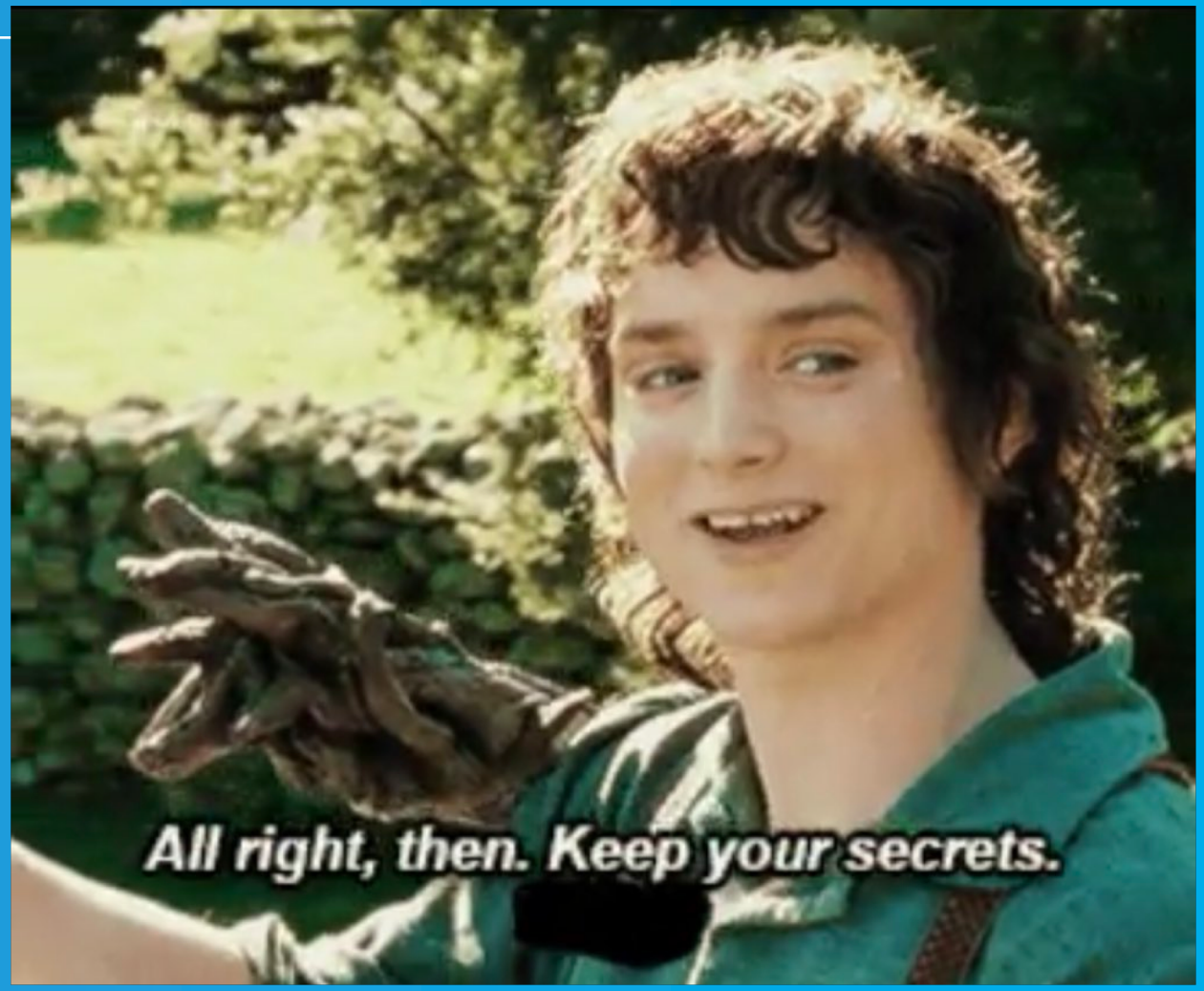
ETCD FINDINGS

2.4K+

- kube-master-1
- kubemaster-etcd
- kubeadm-master2
- k8s_node2
- K8s-cluster-etcd

ETCD RECOMMENDATIONS

- Only API server should have access
- Use TLS for peer communications
- Use certification authentication
- Encrypt data at rest



FINAL THOUGHTS

- Large scale exposure
- Internet exposure is just one piece of the security puzzle
- K8s has lots of security features, understand what they are
- Know what defaults are set with config tools

RESOURCES

1. Kubernetes Illustrated Children's Guide: https://youtu.be/4ht22ReBjno
2. Tesla Exposed Dashboard https://redlock.io/blog/cryptojacking-tesla
3. Weight Watchers Exposed Dashboard https://kromtech.com/blog/security-center/weightwatchers-exposure-a-simple-yet-powerful-lesson-in-cloud-security
4. Censys https://censys.io/
5. Lacework Containers at Risk Report https://info.lacework.com/hubfs/Containers%20At-Risk_%20A%20Review%20of%2021,000%20Cloud%20Environments.pdf
6. CVE-2018-1002105 Github Page https://github.com/kubernetes/kubernetes/issues/71411
7. Shodan https://www.shodan.io/
8. Exposed etcd Clusters Blog https://elweb.co/the-security-footgun-in-etcd/
9. Lacework exposed etcd Clusters Blog https://www.lacework.com/etcd-thousands-of-clusters-open/
10. Lacework Securing K8s Blog https://www.lacework.com/art-into-science-conference-securing-k8s/

QUESTIONS

@laceworklabs

@jameswcondon

james@lacework.com

https://www.lacework.com/blog/

LACEWORK™