
KubeCon
CloudNativeCon
North America 2019

The Devil in the Details: Kubernetes' First Security Assessment

Aaron Small and Jay Beale

Presenting WG Co-Leads

Aaron Small
Google Product Manager
Kubernetes Security
@atlas_hugged

Jay Beale
CTO, InGuardians
Instructor, Black Hat
@jaybeale

Smarter WG Co-Leads

Craig Ingram
Principal Platform Security Engineer, Salesforce
Securing K8s for Heroku **@cji**

Joel Smith
Principal Software Engineer, Red Hat
Member, Product Security Committee

Agenda

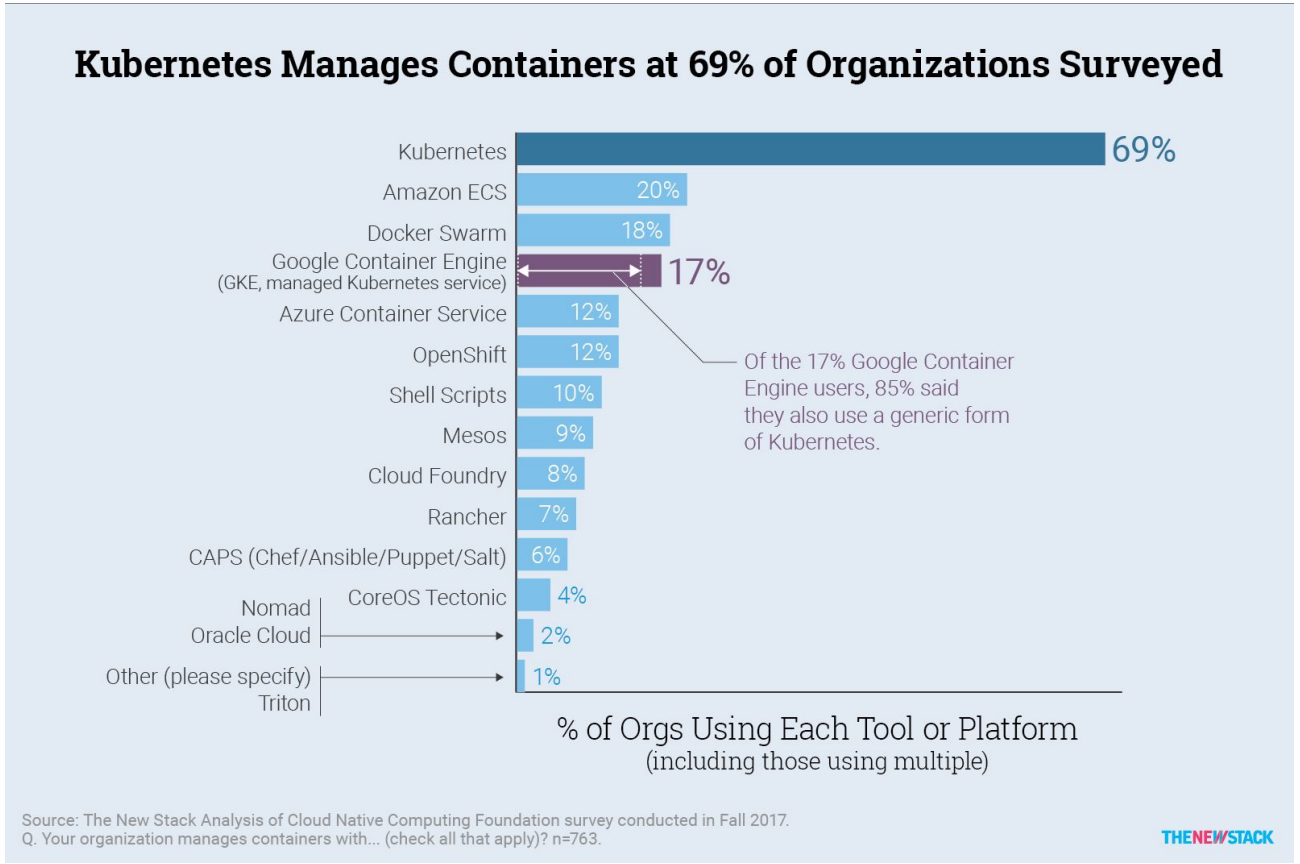
- Why Assess Kubernetes?
- Philosophy
- Attackers' View of Kubernetes
- Approach to the Work
- Threat Model Result Highlights
- Source Assessment Result Highlights
- How you can help

CNCF Sponsorship

- 2018: CNCF Sponsored audits of CoreDNS, Prometheus, and Envoy
  - Quality findings, good bugs, improved security
- 2019: CNCF offers to sponsor audits of graduated projects - Kubernetes volunteers
  - wg-security-audit formed

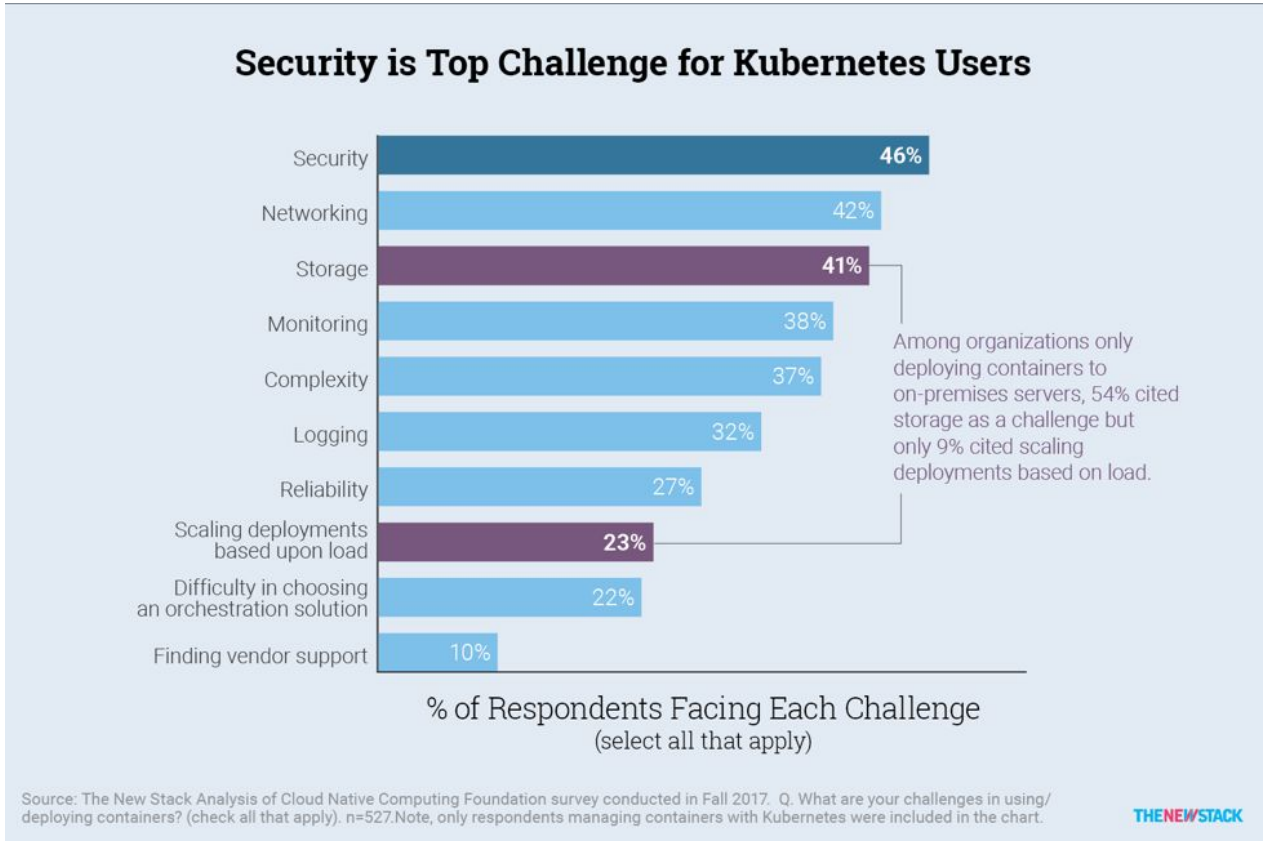
Ecosystem

- Kubernetes is Business Critical



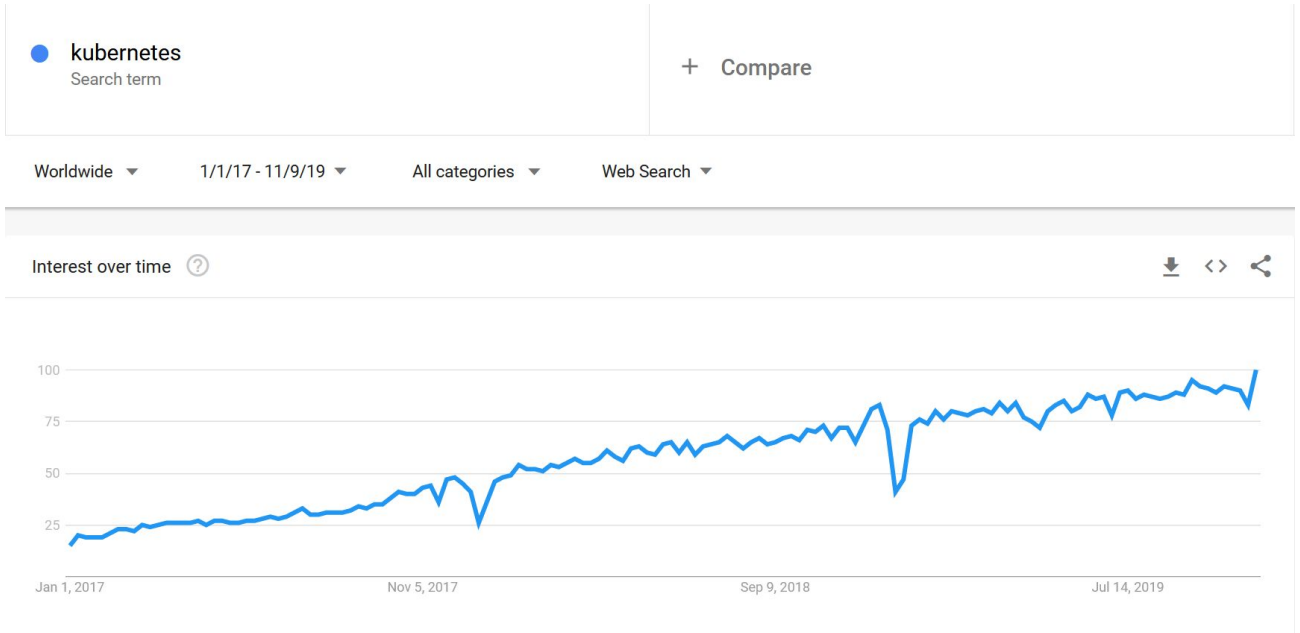
Ecosystem

- Kubernetes is Business Critical
- Security is on everybody's mind



Ecosystem

- Kubernetes is Business Critical
- Security is on everybody's mind
- Interest isn’t exactly declining



Ecosystem

- Kubernetes is Business Critical
- Security is on everybody's mind
- Interest isn't exactly declining
- In the spotlight & under the microscope

https://kubernetes.io/case-studies/

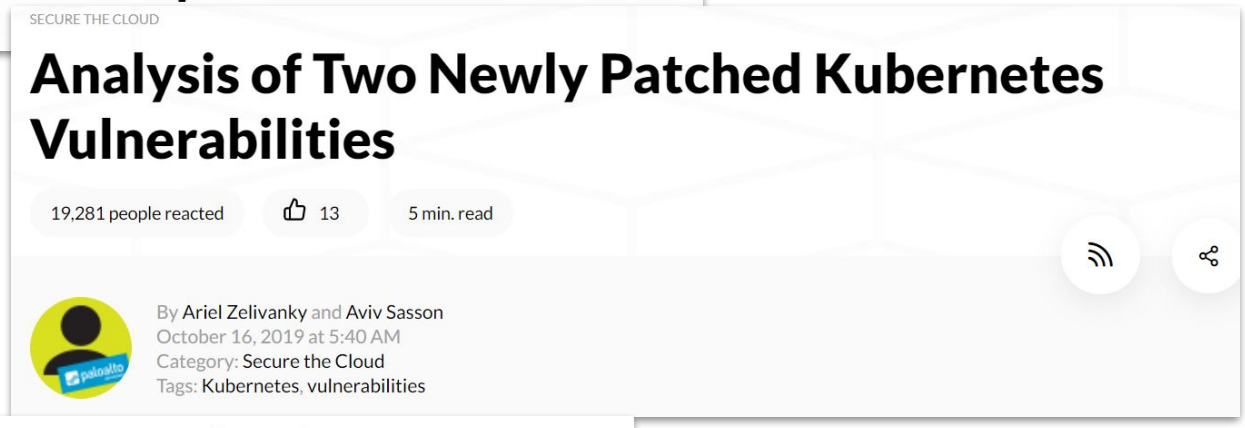
Ecosystem

Vulnerabilities exist and are being exploited in the real world.


KUBERNETES / NETWORKING / SECURITY

Netflix Discovers Severe Kubernetes HTTP/2 Vulnerabilities

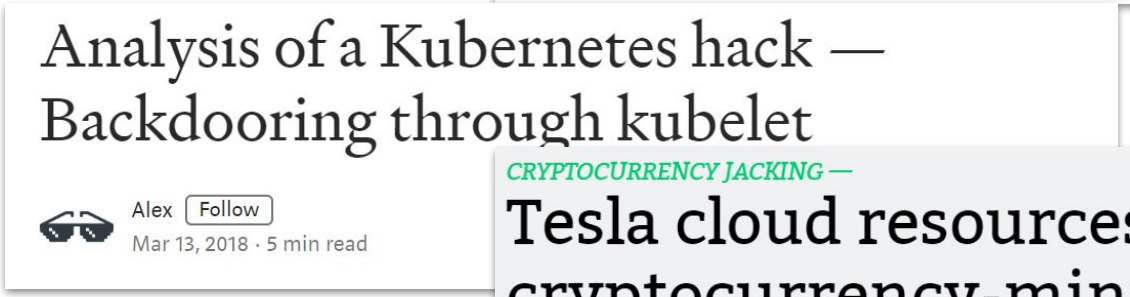
23 Aug 2019 2:10pm, by Jack Wallen


SECURE THE CLOUD

Analysis of Two Newly Patched Kubernetes Vulnerabilities

19,281 people reacted 13 5 min. read

By Ariel Zelivanky and Aviv Sasson
October 16, 2019 at 5:40 AM
Category: Secure the Cloud
Tags: Kubernetes, vulnerabilities


Analysis of a Kubernetes hack — Backdooring through kubelet

Alex Follow
Mar 13, 2018 · 5 min read


CRYPTOCURRENCY JACKING —

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, 11:21 AM

https://medium.com/handy-tech/analysis-of-a-kubernetes-hack-backdooring-through-kubelet-823be5c3d67c
https://blog.paloaltonetworks.com/2019/10/cloud-kubernetes-vulnerabilities/
https://thenewstack.io/netflix-discovers-severe-kubernetes-http-2-vulnerabilities/
https://arstechnica.com/information-technology/2018/02/tesla-cloud-resources-are-hacked-to-run-cryptocurrency-mining-malware/

Philosophy

Audit Kubernetes the Kubernetes way

- Open: Public RFP and selection process
- Transparent: Public audit GitHub repository
- Frugal: specific focuses, allowing for a series of assessments
- Future-focused: Threat model and Attackers Guide

Components to the Assessment

- Traditional Source Assessment
- Attackers Guide
- Threat Model
- Operator White Paper

Attacks on Kubernetes

An Attacker Considers:

- Data Flow
- Critical Components
- Network Isolation
- Trust Boundaries
- Privilege Escalation
- Monkey in the Middle (MitM)
- Secrets

Vantage Points for an Attacker

An attacker on a cluster is trying to compromise and escalate privilege from:

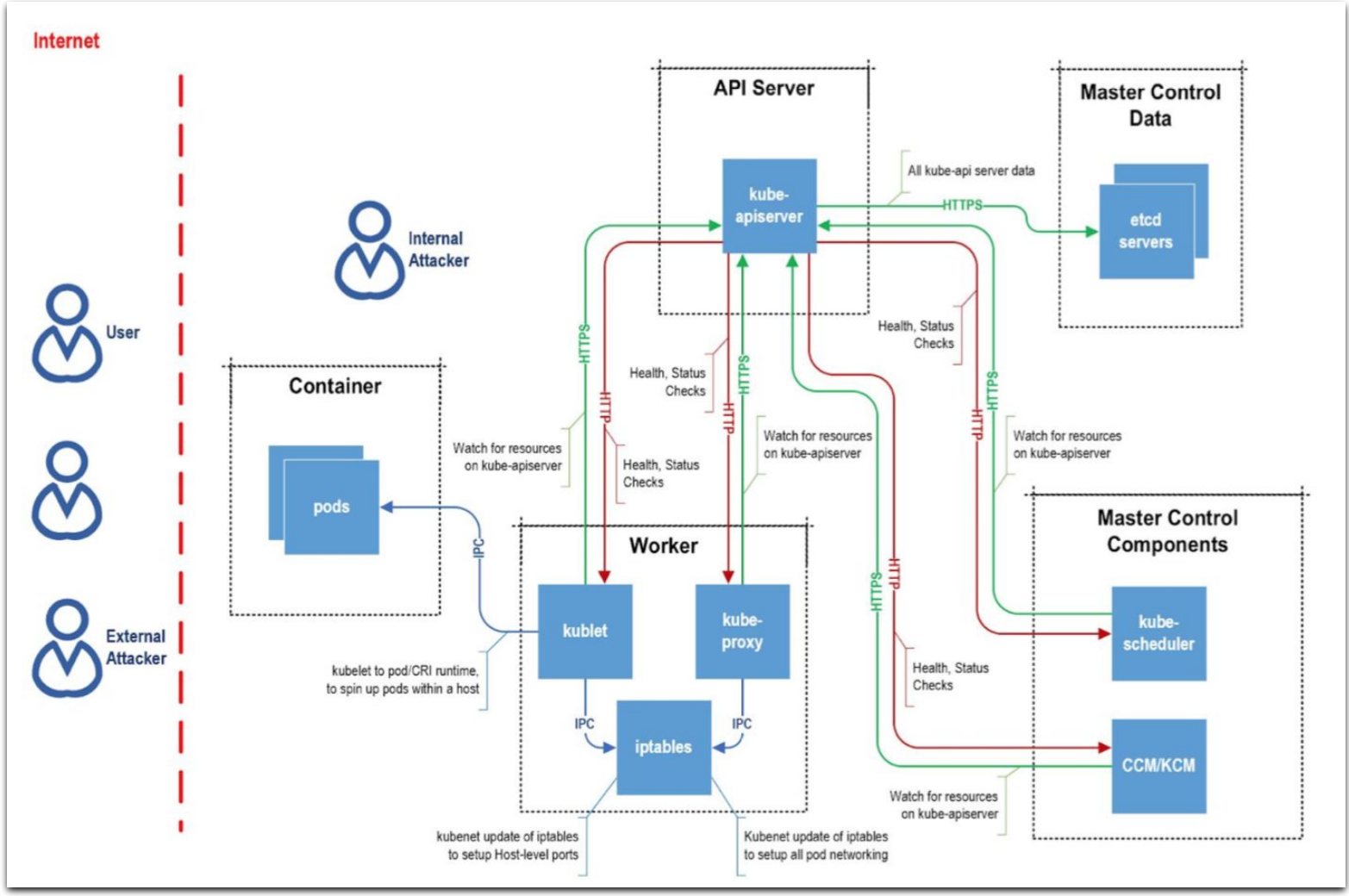
- outside of the cluster.
- inside a container whose program they compromised.
- in a control plane element they've compromised.
- in a node they've escalated privilege on.

Let's look at this from a dataflow and components perspective, using a diagram from the threat model.

An Attacker's view of Kubernetes

- An attacker outside a cluster
  - sees ingress services
  - possibly sees API server
  - less probably sees kubelets, etcd servers, ...

- An attacker inside a cluster:
  - usually sees every component shown here.
  - may have access to the cloud provider APIs.
  - has the opportunity to observe or PitM traffic.
    - note the HTTP flows
    - note unverified endpoints



(Source: Threat Model Deliverable, page 18)

Threat Model

P0 Components

- Kube-apiserver
- Etcd
- Kube-scheduler
- Kube-controller-manager
- Cloud-controller-manager
- Kubelet
- Kube-proxy
- Container Runtime Interface

Control Families

- Networking
- Cryptography
- Authentication
- Authorization
- Secrets Management
- Multi-tenancy

Trust Zones

- Internet
- API Server
- Etcd
- Controller Managers
- Worker Components
- Container Runtime

(Led by Trail of Bits' Stefan Edwards with Working Group participation and contributions from SIG members.)

Threat Model - Highlights

1. **Warn users who configure a security control that will not be enforced**
   - Network policies and pod security policies can silently fail
2. **Require transport encryption, w/ certificate verification**
   - Multiple components use HTTP
   - Multiple components elect not to verify certificate validity
3. **Prevent node compromises from leading to cluster compromise**
   - Host access gives access to command-line arguments, logs, …
4. **Provide auditing information in a unified fashion**
   - Allow a trace of a user's/attacker's actions through the system.
5. **Separate privilege levels among controllers**

Source Assessment

- Initial best-effort vulnerability audit. Time split between:
  - Vulnerability research
  - Threat model
  - Whitepaper
- Discovered 37 vulnerabilities
- Reported vulnerabilities into the project

Source Assessment - Highlights

Issue	Severity	Issue #	CVE
Non-authenticated HTTPS Connections	High	#81112	
Certificate Revocation unsupported	High	#18982	
PodSecurityPolicy Bypass (hostPath Volumes via PVs)	High	#81110	
TOCTOU Race Condition: Kubelet	High	#81113	
Improperly-patched kubectl cp directory traversal	High	PR 76788	CVE-2019-11249
System logs contain bearer tokens, iSCSI credentials, ...	Medium	#81114 & #81130	CVE-2019-11250

> Overall, Kubernetes is a large system with significant operational complexity. The assessment team **found configuration and deployment of Kubernetes to be non-trivial**, with certain components having **confusing default settings**, missing operational controls, and **implicitly defined security controls**. Also, the state of the Kubernetes codebase has significant room for improvement. The codebase is large and complex, with **large sections of code containing minimal documentation and numerous dependencies**, including systems external to Kubernetes. There are **many cases of logic re-implementation** within the codebase which could be centralized into supporting libraries to reduce complexity, facilitate easier patching, and reduce the burden of documentation across disparate areas of the codebase.

Call for Action

Systemic issues need you!

- Refactor one set of logic re-implementations to a library function.
- Fix an instance of “user inaccurately believed a control was activated.”
- Propose privilege separations for the controllers.
- Develop a better default audit policy.
- Improve at least one case of weak file permissions.
- Propose standards or create developer docs to avoid this audit’s vulns.
- Attack Kubernetes and report your findings: https://bit.ly/33AcXWL
- Participate in the next audit: Stay tuned!

Thank You!

- Working Group Co-Leads
- Chris Aniszczyk, CNCF
- Threat model volunteers
  - Tim Allclair
  - Tim Hockin
  - Walter Fender
  - Bobby Salamat
  - Dawn Chen
  - Mike Spreitzer
- Trail of Bits
- Atredis Partners

- You! In Advance! (Future Kubernetes hackers in the audience)

See Also

“Walls within Walls: What if Your Attacker Knows Parkour” https://bit.ly/2QfYcoa
Tim Alclair and Greg Castle : Tue 3:20pm

“Piloting Around the Rocks: Avoiding Threats in Kubernetes” https://bit.ly/36XLAbc
Robert Tonic and Stefan Edwards : Wed 2:25pm

“Hello from the Other Side: Dispatches from a Kubernetes Attacker” https://bit.ly/2NBpe7Y
Ian Coldwater : Thur 9:22 am

“Attacking and Defending Kubernetes Clusters: A Guided Tour” https://bit.ly/36Xb0G0
Brad Geesaman, Jimmy Mesta, Tabitha Sable, Peter Benjamin : Thur 4:25pm

“Kubernetes Practical Attack and Defense” https://bit.ly/2K93TAA
Jay Beale : Blue Hat Oct 31, 2019

Questions?

Resources

- **Kubernetes Security Assessment**
  - Reports: **https://bit.ly/2NPpaAc**
  - Issues: **https://bit.ly/2WY3RAR**
- **Previous CNCF Security Assessments**
  - CoreDNS: **https://bit.ly/32ASRKF**
  - Envoy: **https://bit.ly/32t2mvH**
  - Prometheus: **https://bit.ly/33xwKGB**
- **Get in touch with us**
  - Slack channel: **https://bit.ly/2q0WmwX**
    (see “Joining Kubernetes Slack” on right as necessary)
  - Git Repo: **https://bit.ly/2Q6tnCr**

- Report a Vulnerability: https://bit.ly/33AcXWL
- Trail of Bits audit repo: https://bit.ly/36IdTue

Join Kubernetes Slack:

- Review the Guidelines **https://bit.ly/2D52yHd**
- Get an automatic invite **https://slack.k8s.io/**