

# Container Infrastructure Analysis with kube-hunter

---



**Zach Roof**

Lead Security Engineer

@zachroofsec [www.zachroofsec.com](http://www.zachroofsec.com)





kube-hunter





# kube-hunter

Creator: Aqua Security



**kube-hunter is an open-source tool that hunts for  
Kubernetes security issues**





## Prerequisites

- Basic Docker knowledge
- <https://app.pluralsight.com/library/courses/getting-started-docker>
- Basic Kubernetes (K8s) knowledge
- <https://app.pluralsight.com/library/courses/kubernetes-getting-started>
- Links
- <https://github.com/zachroofsec/kube-hunter-tutorial>





## Documentation

- [github.com/aquasecurity/kube-hunter](https://github.com/aquasecurity/kube-hunter)

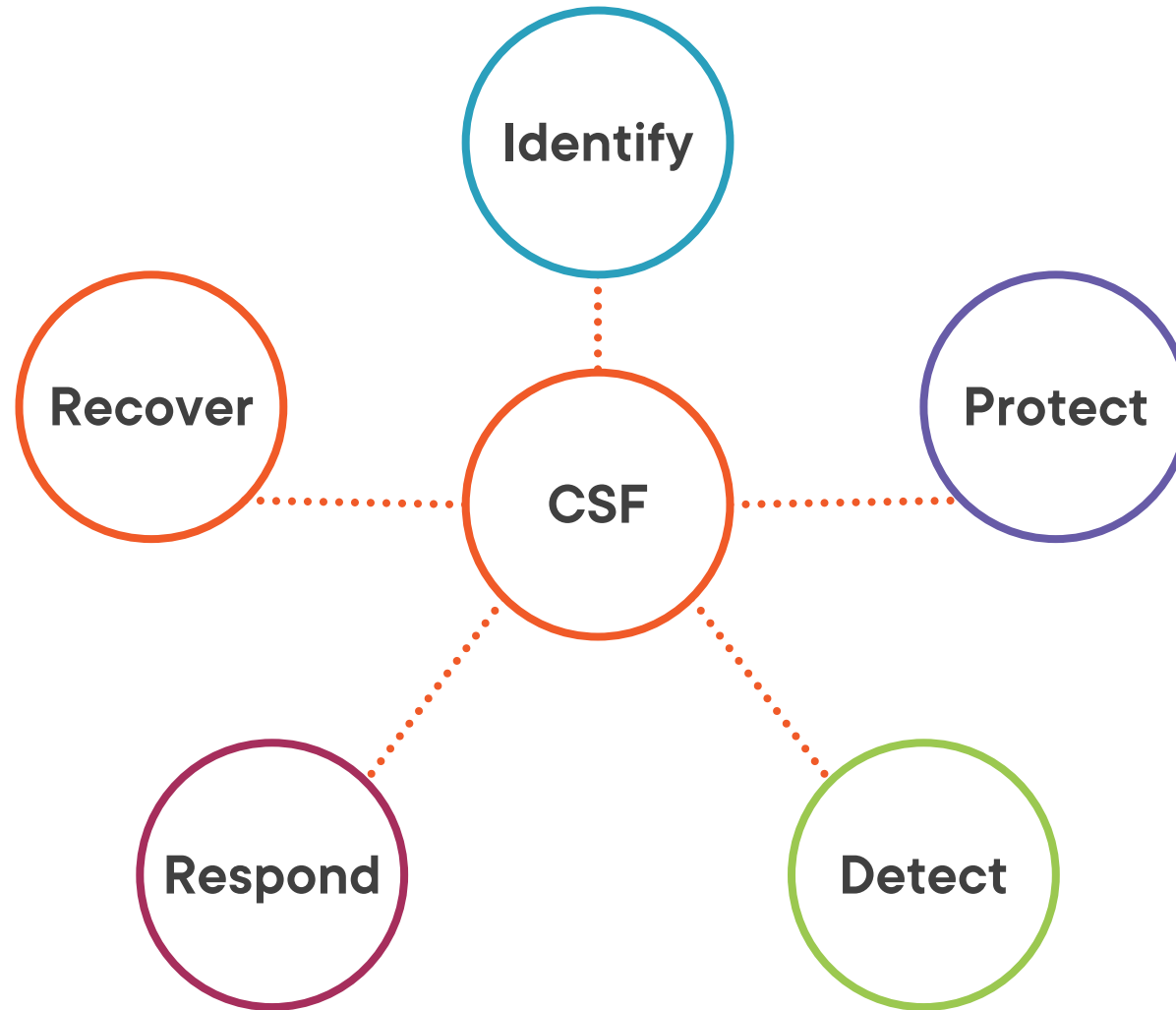
## Scan perspectives

- Remote
- Server
- Cluster

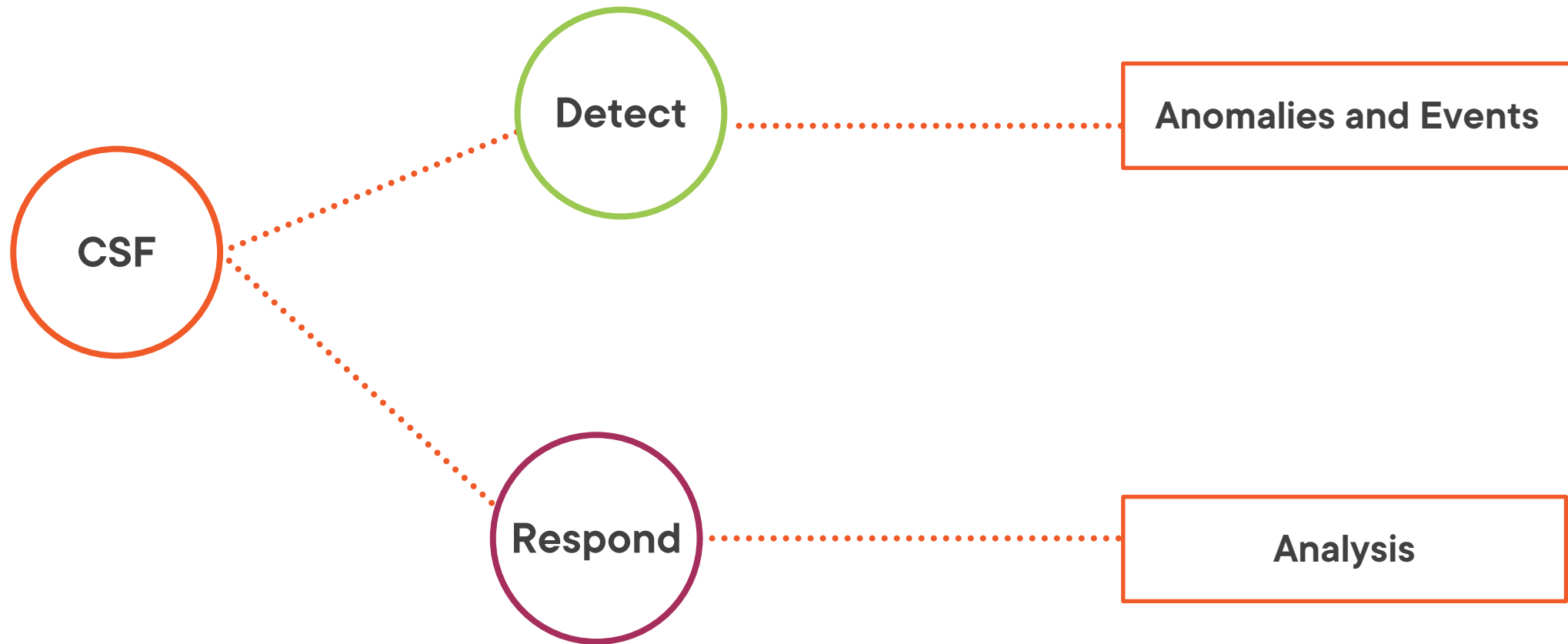
## Active mode vs passive mode



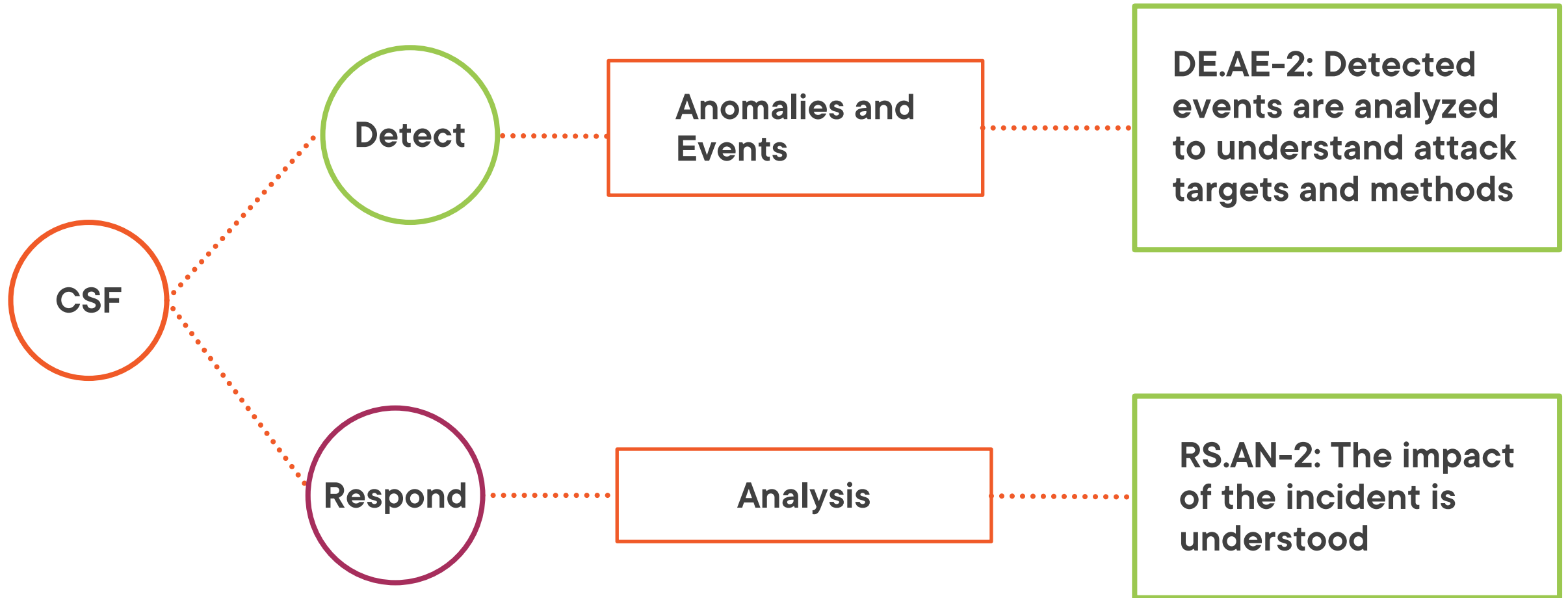
# NIST Cybersecurity Framework (Core)



# NIST Cybersecurity Framework



# NIST Cybersecurity Framework





# MITRE ATT&CK

## Data Analysis Type

**Network Analysis**

**Infrastructure Analysis**

**Application Analysis**

**OS Analysis**

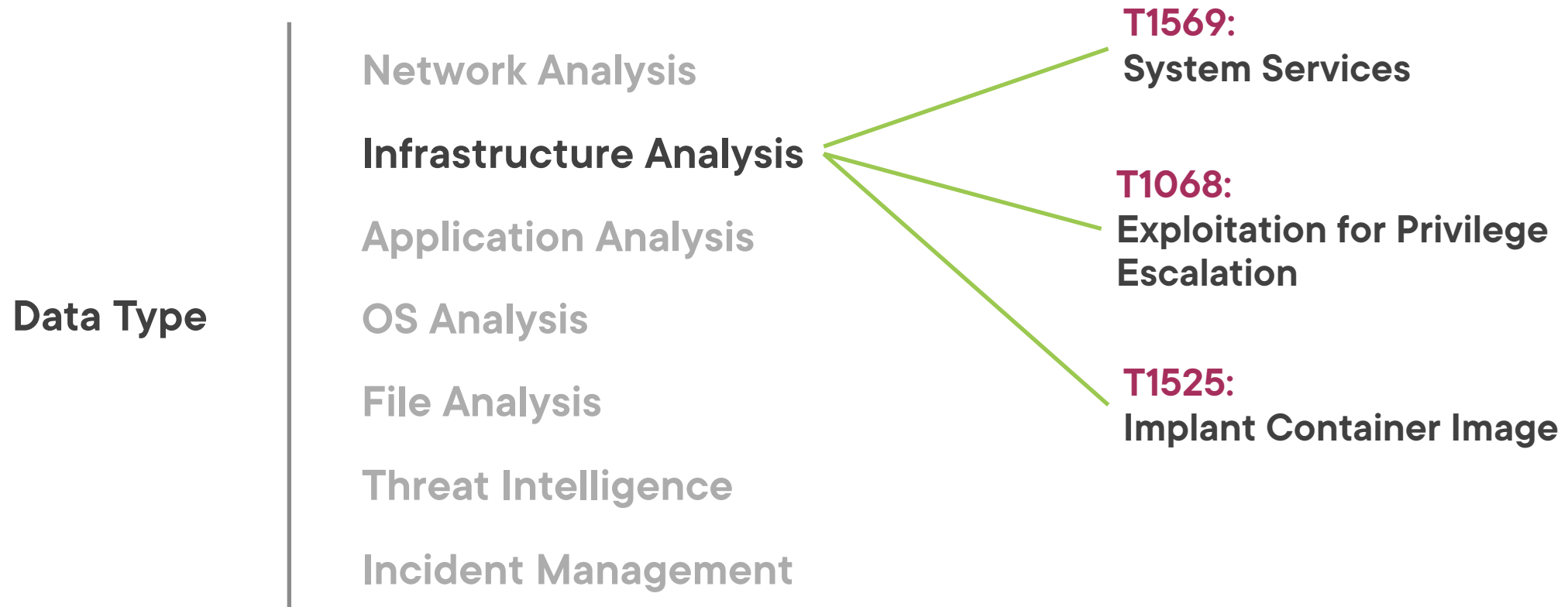
**File Analysis**

**Threat Intelligence**

**Incident Management**



# MITRE ATT&CK



# MITRE SHIELD

## T1569:

### System Services

**DTE0003 - API Monitoring:** A defender can monitor operating system functions calls to look for adversary use and/or abuse. (DUC0032)

## T1068:

### Exploitation for Privilege Escalation

**DTE0001 - Admin Access:** A defender can configure system users to not have admin access in order to ensure privilege escalation requires exploitation (DUC0055)

## T1525:

### Implant Container Image

**DTE0007 - Behavioral Analytics:** A defender can monitor user interactions with images and containers to identify ones that are added or altered anomalously. (DUC0168)

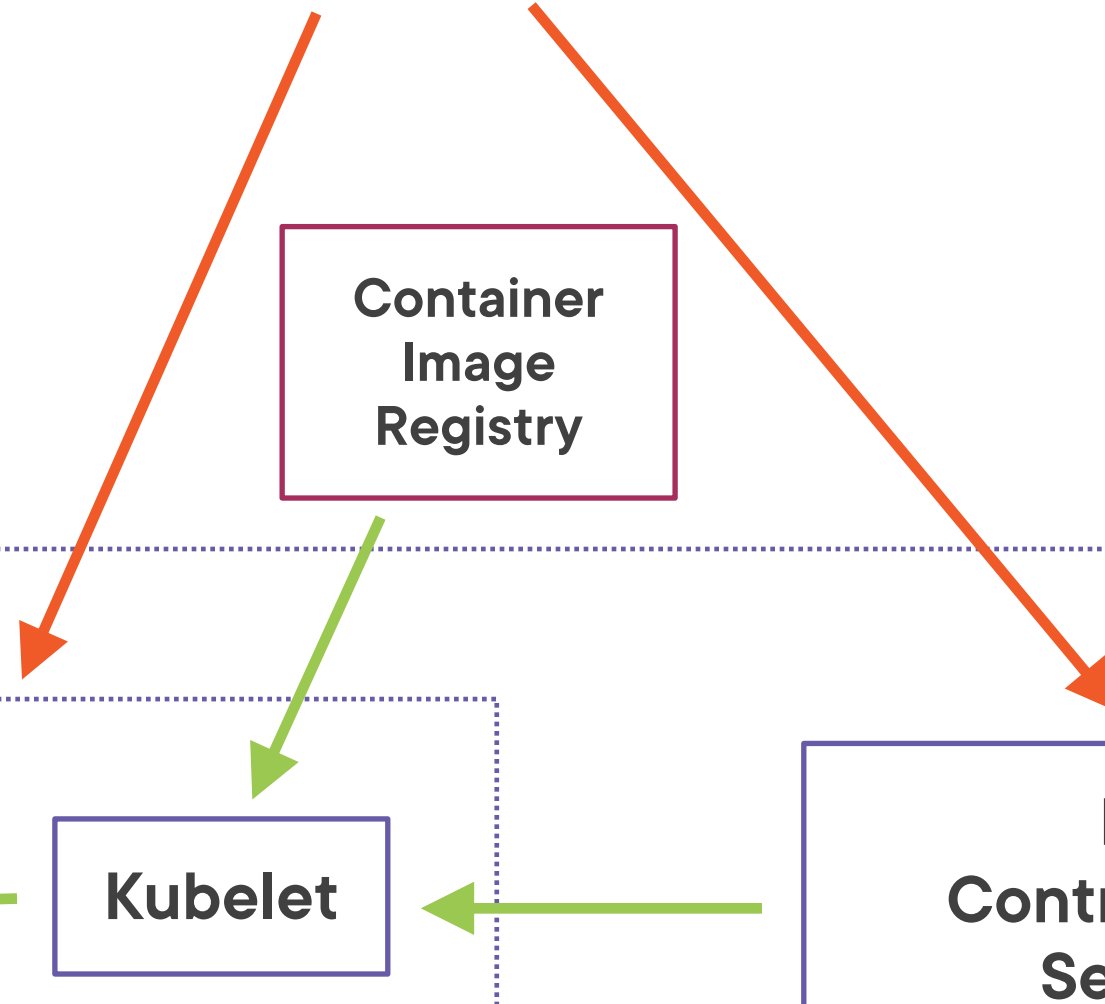
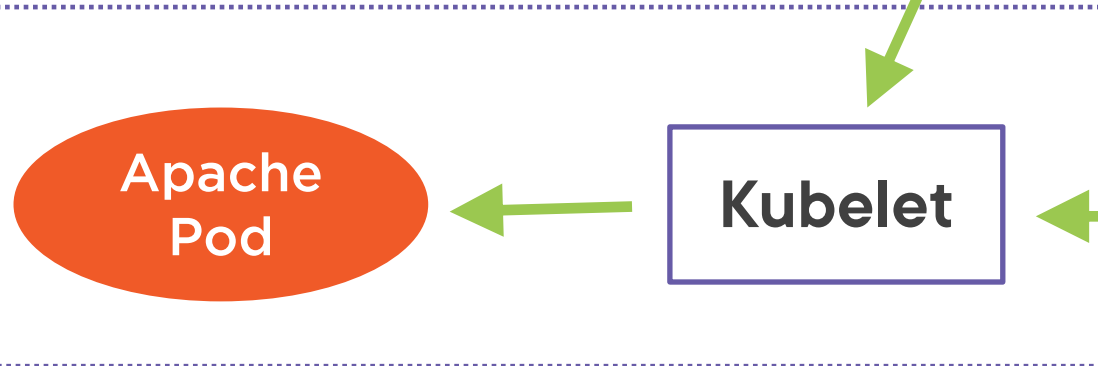


## Demo Environment



## Data Center

### K8s Worker Nodes



# Demo



- Review kube-hunter's command line flags
- Audit local Kubernetes cluster
- Review kube-hunter findings



# Demo



- Review kube-hunter's command line flags
- Audit local Kubernetes cluster
- Review kube-hunter findings
  - Information disclosure
  - Recon
  - Anonymous authentication
  - Connect
  - Remote code execution
  - Take action



# Demo



- Leverage nmap to hunt for vulnerable Kubernetes services
- Hunt for vulnerabilities via the /pods metadata endpoint
- Use a kubelet vulnerability to do an investigation



# Demo

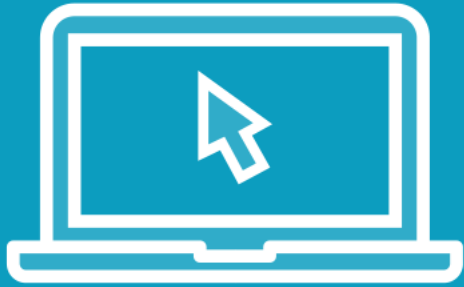


- Leverage nmap to hunt for vulnerable Kubernetes services
  - Found heartbleed
- Hunt for vulnerabilities via the /pods metadata endpoint
  - /host mount is exposed within pod
- Use a kubelet vulnerability to do an investigation
  - Executed shhgkit within pod
  - shhgkit found registry credentials within /host





# Demo



- Inspect container image vulnerabilities with Trivy
- Look for signs of image modification with docker history



# Demo



- Inspect container image vulnerabilities with Trivy
  - Found heartbleed
- Looked for signs of image modification with docker history
  - Docker history cant be completely trusted
- Container Infrastructure Analysis With Trivy
  - Advanced checks for image tampering
  - Vulnerability scanning with Trivy



# Demo



- How could we prevent this attack?
- Kubelet hardening
- Pod Security Policies
- Attempt to launch insecure Pod



# Additional Resources

## Capabilities

- [kube-hunter README](#)
- [kube-hunter modules](#)

## Related Information

- [Container Infrastructure Analysis With Trivy](#)
- [kubeletctl](#)
- [Pod Security Policies](#)
- [kube-bench](#)



# Container Infrastructure Analysis with kube-hunter

---



**Zach Roof**

Lead Security Engineer

@zachroofsec [www.zachroofsec.com](http://www.zachroofsec.com)



## Investigation Chain

### kube-hunter

- Findings:
  - kubelet RCE
  - kubelet /pods

### nmap

- Findings:
  - heartbleed

### kubelet /pods

- Findings
  - Docker image name
  - host filesystem mounted within Pod

### kubelet RCE

- Findings
  - Docker credentials within host filesystem

### Defender

- Container image implanted by attacker?

### Trivy

- Findings
  - heartbleed in docker image

