BANZAICLOUD

Improve Kubernetes Security

Péter **Balogh**

peter.balogh@banzaicloud.com

June 17, 2019

Kubernetes

> “Kubernetes is a portable, extensible open-source platform for managing containerized workloads and services, that facilitates both declarative configuration and automation. It has a large, rapidly growing ecosystem. Kubernetes services, support, and tools are widely available.”

The most painful vulnerabilities:

-	K8s	CVE-2018-1002105
-	runC	CVE-2019-5736
-	alpine	CVE-2019-5021

What can we do?

- **RBAC**
  - PoLP (Principle of Least Privilege)
- **Network Security**
  - Namespace isolation (NetworkPolicy)
  - Encrypted communication
- **Container Image Security**
  - Trusted store (signed images)
  - Deploy time vulnerability scan
- **Storing Secrets**
  - Using Hashicorp Vault instead of K8s secrets
- **Admission plugins**
  - AlwaysPullImages
  - PodSecurityPolicy
- **Audit log**
  - Tune logging via Policy file
- **Node security**
  - kubernetes
  - container runtime
  - installed packages

As we do in Banzai Cloud

Vulnerability scans: Anchore Engine

Container image scans

Policy evaluation

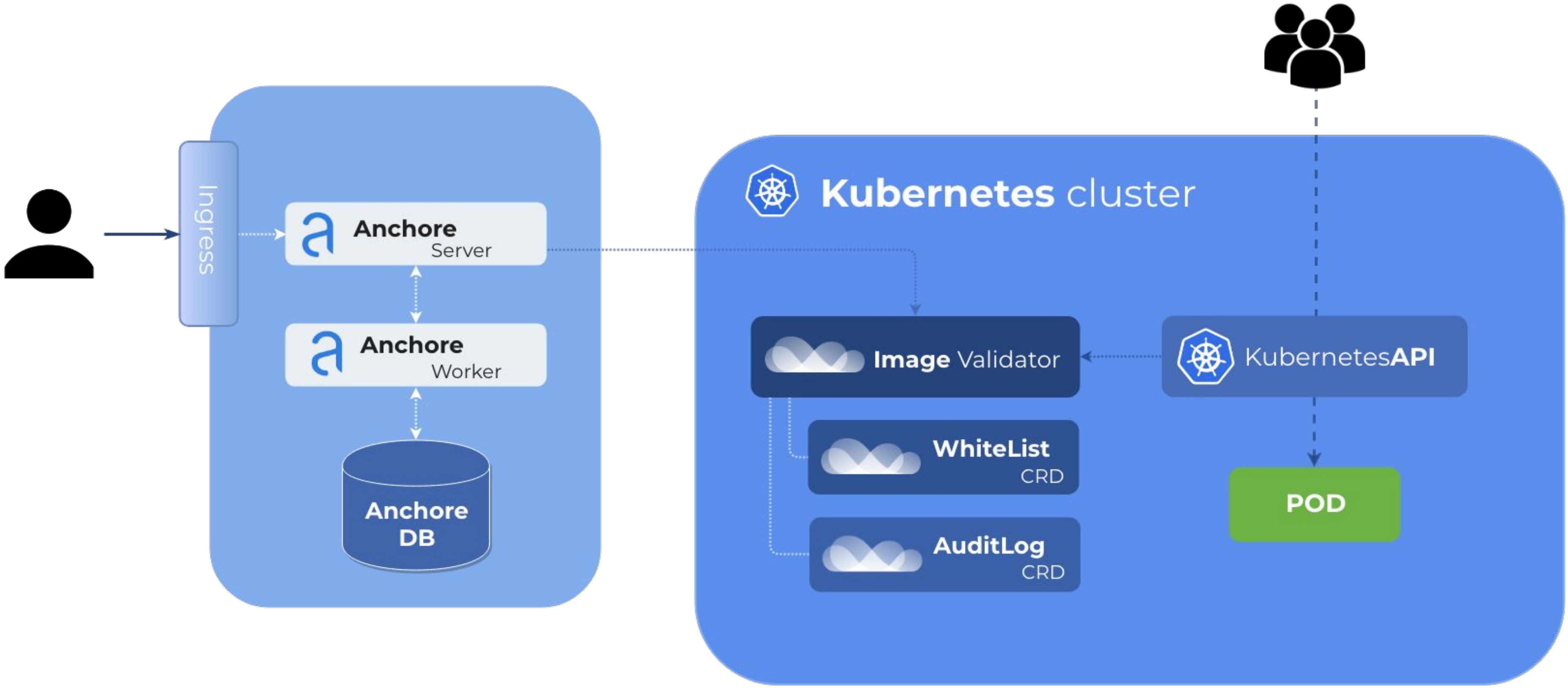
Integrated into deployment flow

https://anchore.com/engine/

https://github.com/banzaicloud/anchore-image-validator

https://banzaicloud.com/tags/vulnerability/

Vulnerability scans: Anchore Image Validator



Secret management: Vault

Bank Vaults (Vault swiss-army knife and operator)

Automatic unsealing, token renewal

Kubernetes support

Secret injection (mutating webhook)

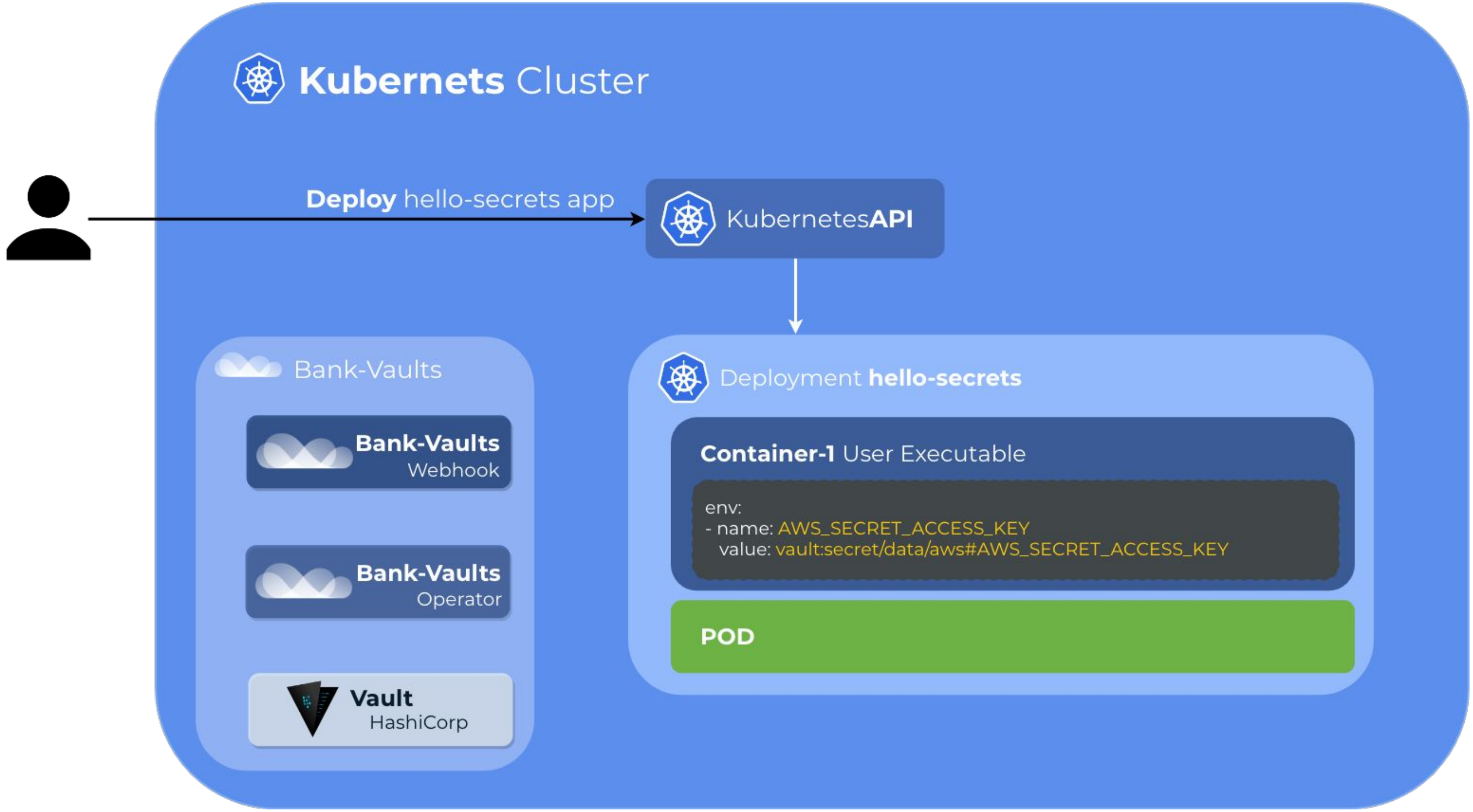
https://www.vaultproject.io/

https://github.com/banzaicloud/bank-vaults

HashiCorp
Vault

BANZAICLOUD

Secret management: Vault secret injection



```
env:
- name: AWS_SECRET_ACCESS_KEY
  value: vault:secret/data/aws#AWS_SECRET_ACCESS_KEY
```

Service Mesh: Istio

Securely connect services within (and outside of) the mesh

Control access through various policies

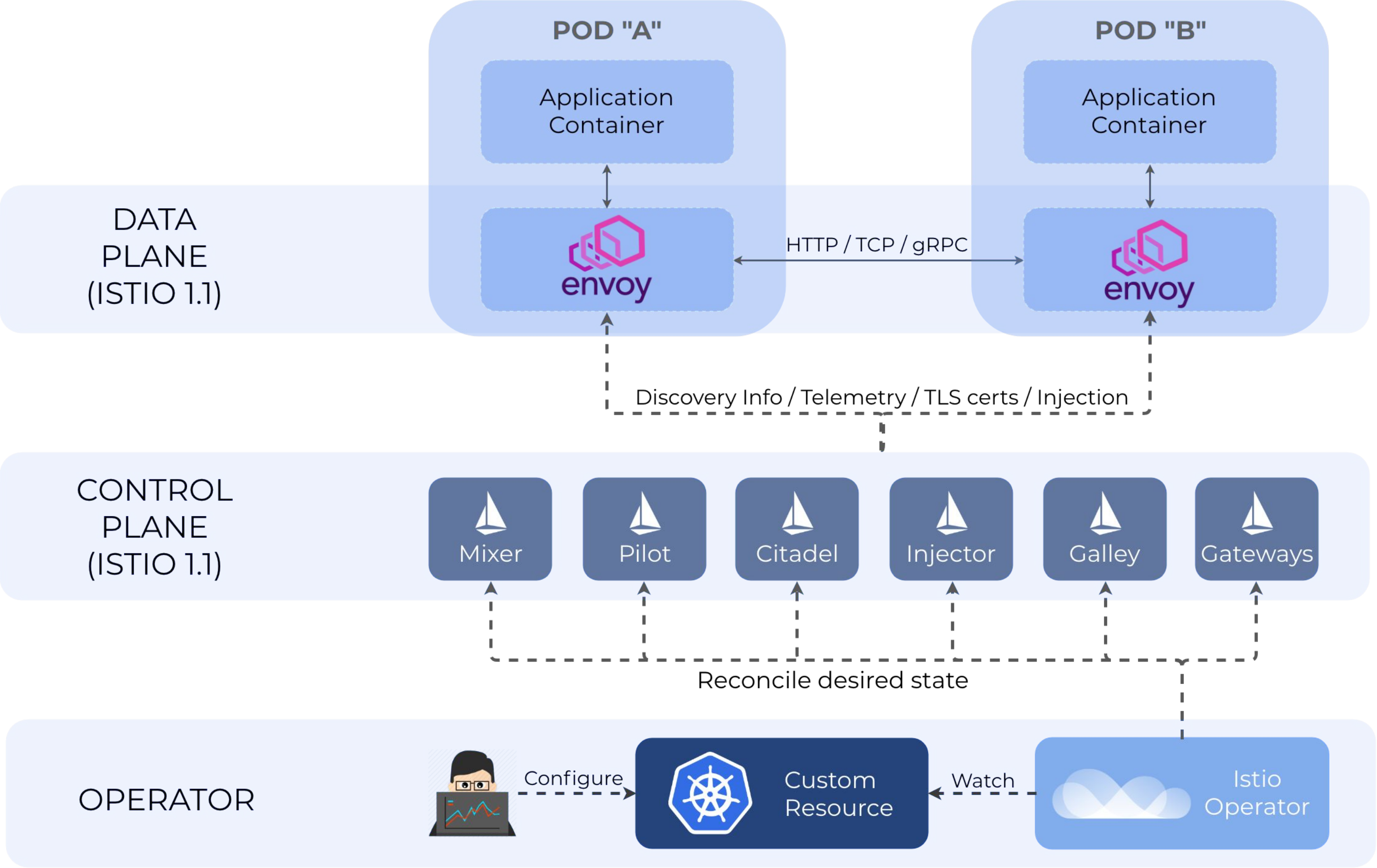
Observe and trace traffic between services

https://istio.io/

https://github.com/banzaicloud/istio-operator

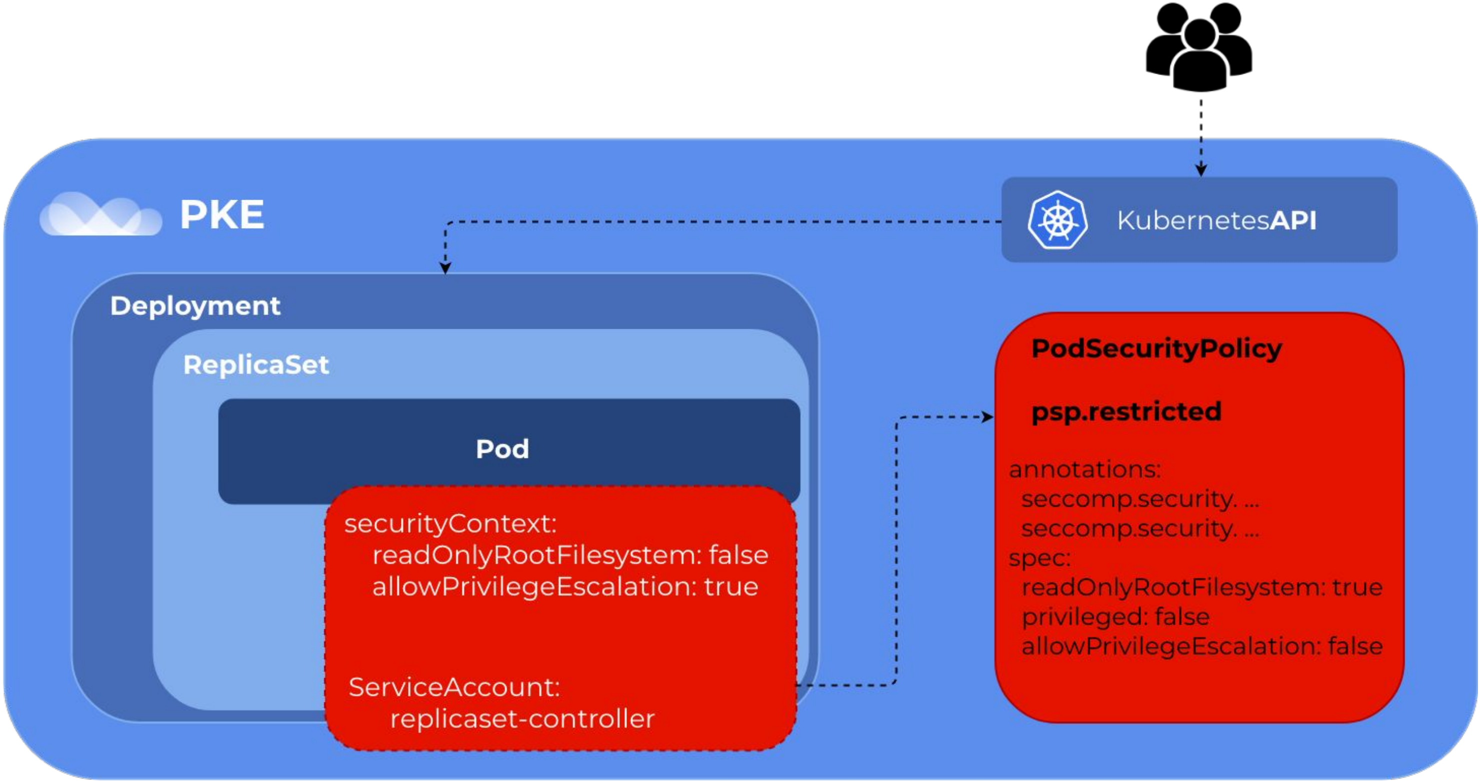
BANZAICLOUD

Service Mesh: Istio Operator



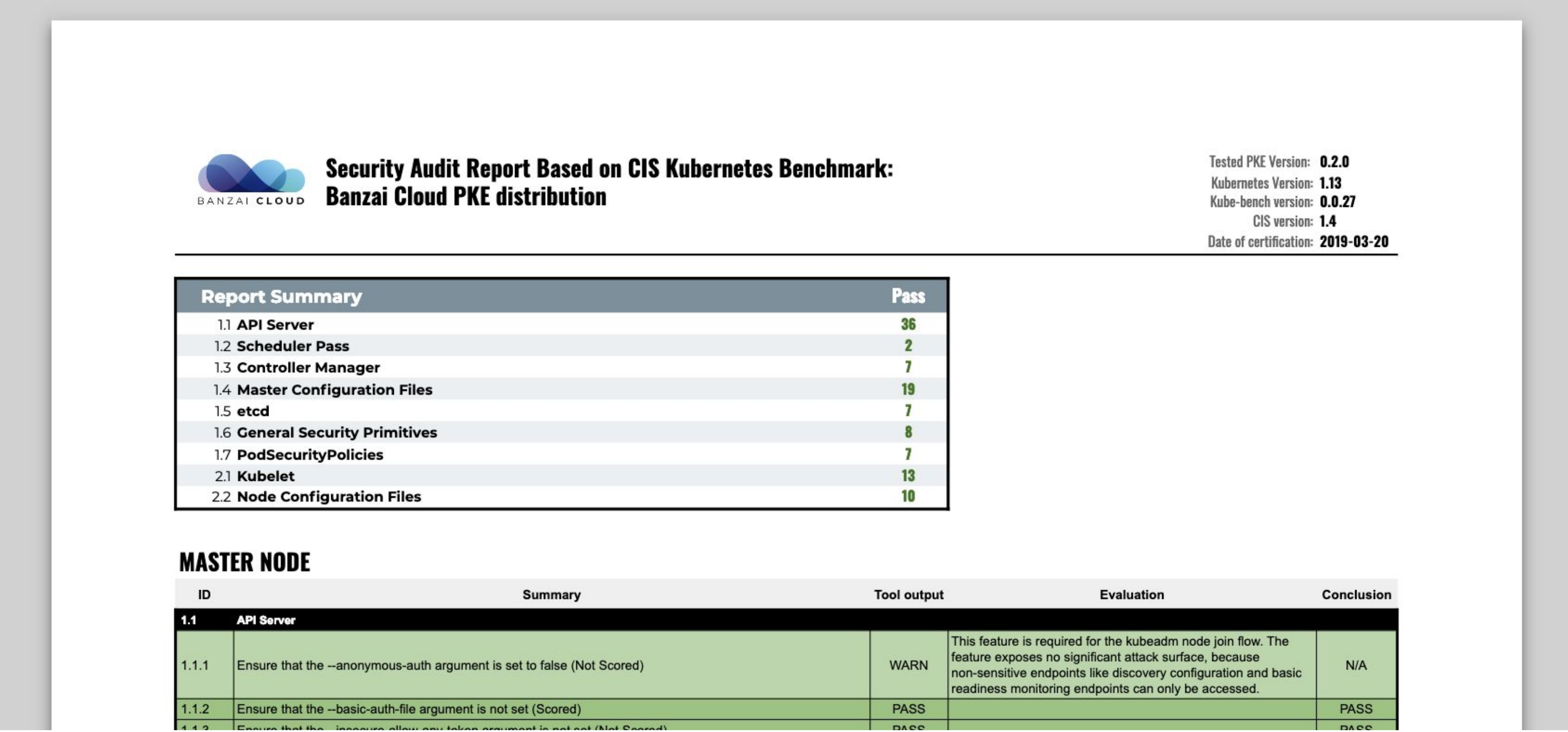
BANZAICLOUD

PodSecurityPolicy in PKE (own K8s distribution)



BANZAICLOUD

PKE Kubernetes CIS benchmark



BANZAI CLOUD

Security Audit Report Based on CIS Kubernetes Benchmark: Banzai Cloud PKE distribution

Tested PKE Version:	0.2.0
Kubernetes Version:	1.13
Kube-bench version:	0.0.27
CIS version:	1.4
Date of certification:	2019-03-20

Report Summary		Pass
1.1	API Server	36
1.2	Scheduler Pass	2
1.3	Controller Manager	7
1.4	Master Configuration Files	19
1.5	etcd	7
1.6	General Security Primitives	8
1.7	PodSecurityPolicies	7
2.1	Kubelet	13
2.2	Node Configuration Files	10

MASTER NODE

ID	Summary	Tool output	Evaluation	Conclusion
1.1	API Server			
1.1.1	Ensure that the --anonymous-auth argument is set to false (Not Scored)	WARN	This feature is required for the kubeadm node join flow. The feature exposes no significant attack surface, because non-sensitive endpoints like discovery configuration and basic readiness monitoring endpoints can only be accessed.	N/A
1.1.2	Ensure that the --basic-auth-file argument is not set (Scored)	PASS		PASS
1.1.3	Ensure that the --insecure-allow-any-token argument is not set (Not Scored)	PASS		PASS

Questions?!

BANZAI**CLOUD**