SYSDIG WEBINARS

Become a Certified K8s Security Specialist (CKS) in 2022!

How to Pass with Saiyam Pathak, CNCF Ambassador

SAIYAM PATHAK

CNCF Ambassador &
Director of Technical Evangelism at Civo

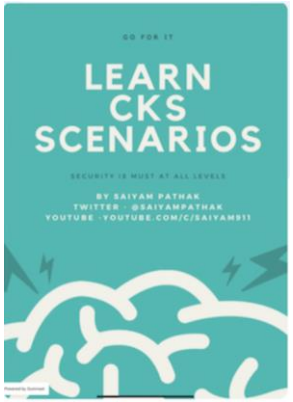
sysdig

Director of technical evangelism, Civo
CNCF Ambassador
CK{A,AD,S}
KCNA SME

@saiyampathak

https://saiyampathak.com/youtube

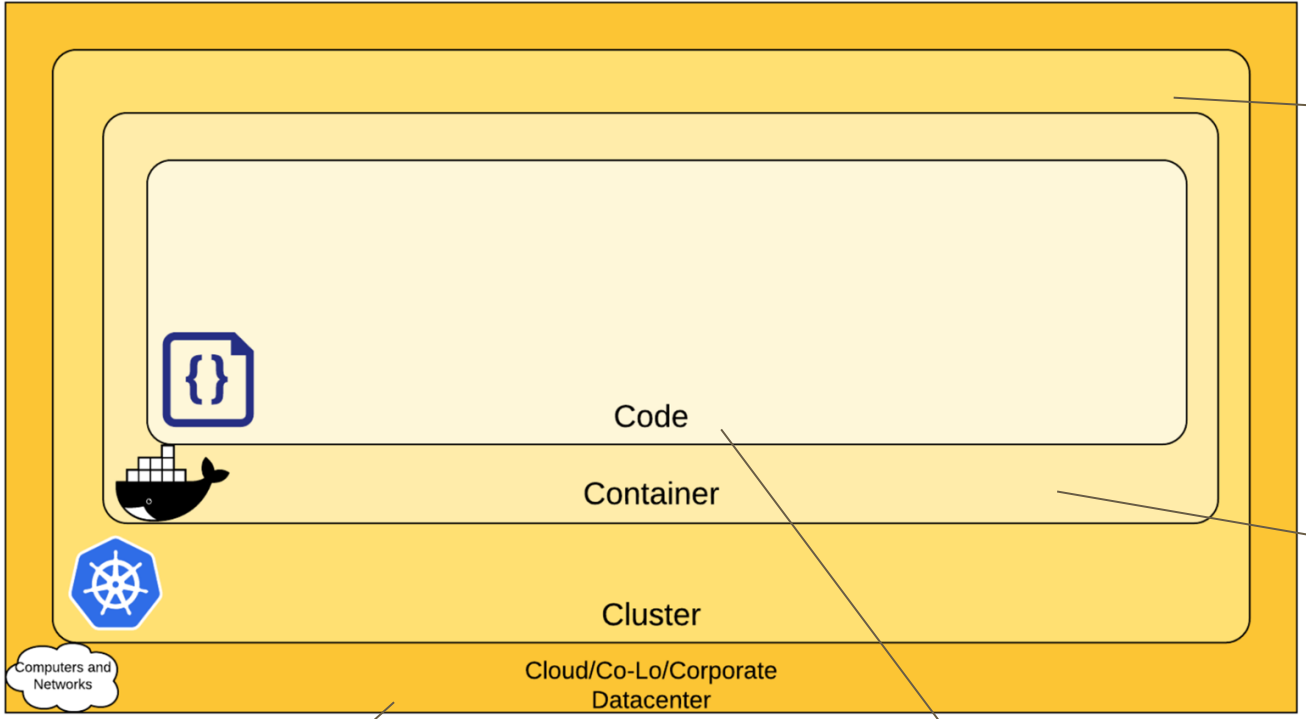
https://saiyampathak.com/discord



Author - CKS scenarios
Kubernetes CKS certification

Agenda

- An overview of cloud-native security
- Quick look at Falco
- CKS exam details and focus areas
- Tips and tricks that can help you prior to and during the exam
- Learning resources
- Playground and Demo
- Q/A

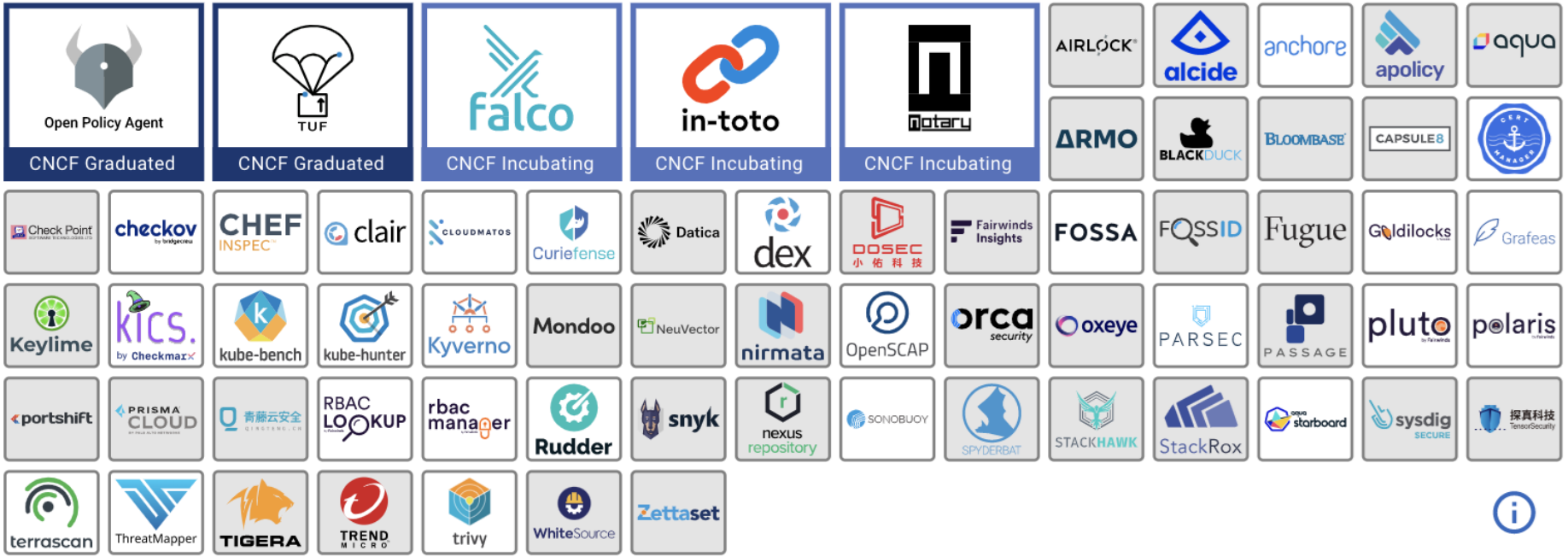


A A A
CIS scans
NSA hardening guide
Network policies
Pod security
Policies tooling
TLS
Secrets and encryption

Container scanning
Signed images
Dockerfile best practices
No privileged users

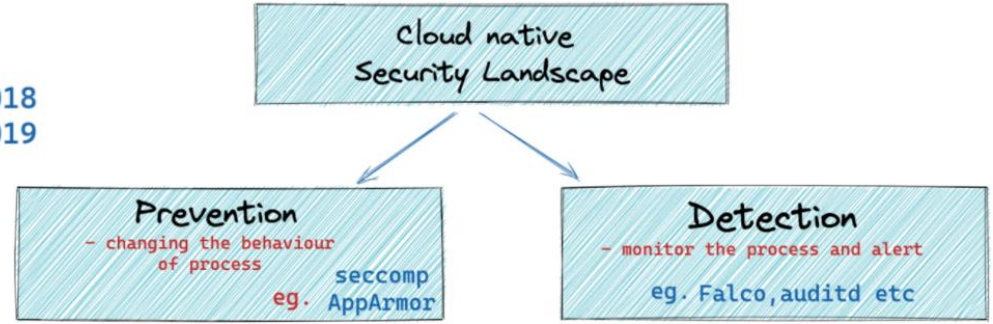
Exposing nodes to internet
limiting control plane access
etcd encryption
Host OS scans

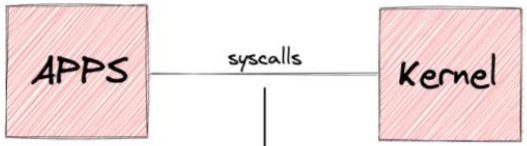
static code analysis
TLS and mTLS between services
limiting port ranges
Dependency scanning
Attack tooling


Open Policy Agent
CNCF Graduated
TUF
CNCF Graduated
falco
CNCF Incubating
in-toto
CNCF Incubating
Notary
CNCF Incubating
AIRLOCK
alcide
anchore
apolicy
aqua
ARMO
BLACKDUCK
BLOOMBASE
CAPSULE8
Check Point
checkov
CHEF INSPEC
clair
CLOUDMATOS
Curiefense
Datica
dex
DOSEC
Fairwinds Insights
FOSSA
FOSSID
Fugue
Goldilocks
Grafeas
Keylime
kics by Checkmarx
kube-bench
kube-hunter
Kyverno
Mondoo
NeuVector
nirmata
OpenSCAP
orca security
oxeye
PARSEC
PASSAGE
pluto
polaris
portshift
PRISMA CLOUD
青藤云安全
RBAC LOOKUP
rbac manager
Rudder
snyk
nexus repository
SONOBUOY
SPYDERBAT
STACKHAWK
StackRox
starboard
sysdig SECURE
探真科技
terrascan
ThreatMapper
TIGERA
TREND MICRO
trivy
WhiteSource
Zettaset

Falco, the cloud-native runtime security project,
is the de facto Kubernetes threat detection engine

Created - 2016
Donated to CNCF - 2018
CNCF Incubating - 2019

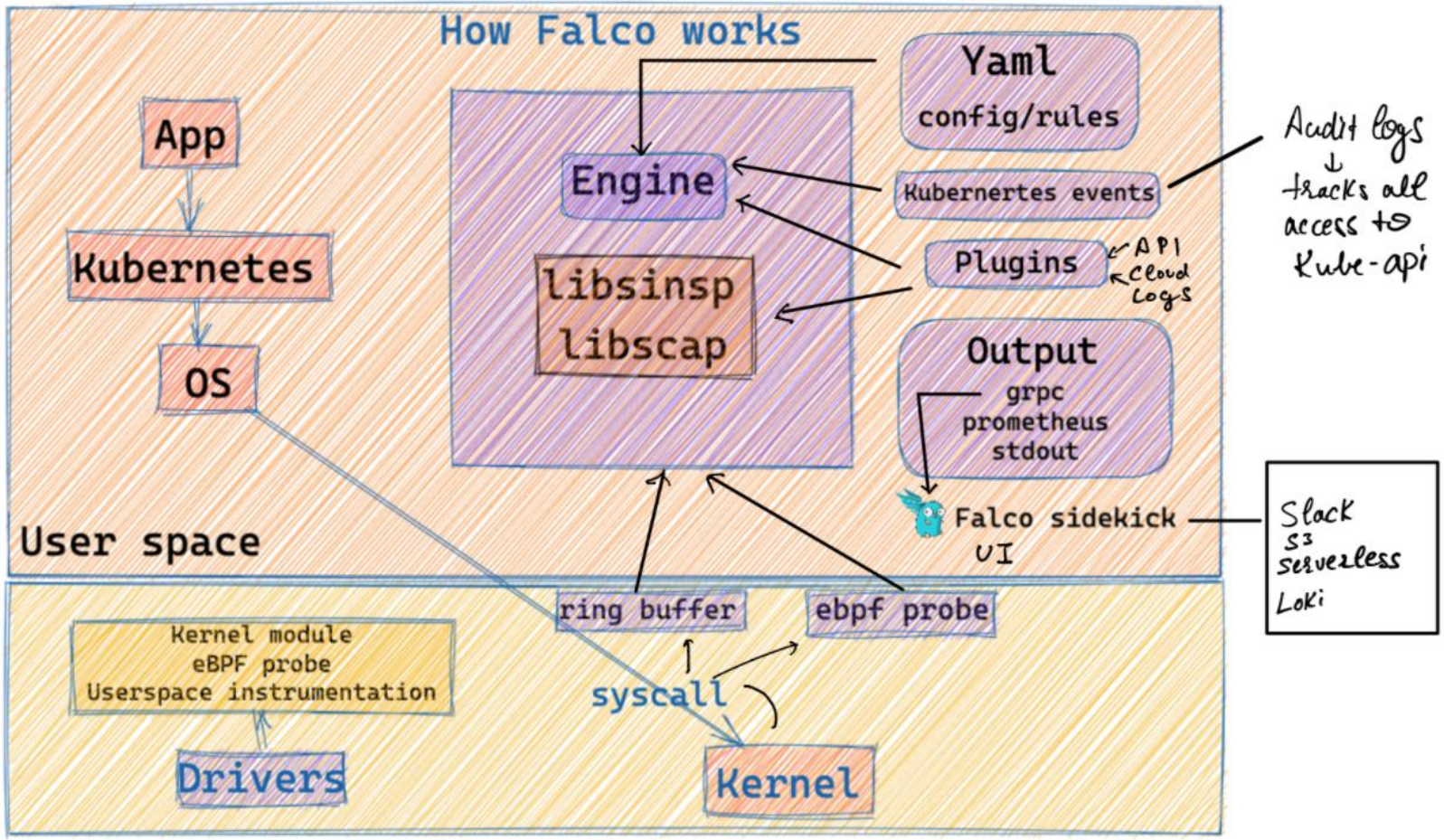




FALCO

- Parse system calls
- Checks against rules defined
- Alerts on rules violation

Stats
- 4200+ stars
- 120+ contributors
- 35M+ Pulls
- 3.5M+ sidekick


How Falco works
Yaml
config/rules
App
Engine
Kubernertes events
Audit logs
↓
tracks all
access to
Kube-api
Kubernetes
Plugins
API
Cloud
Logs
libsinsp
libscap
OS
Output
grpc
prometheus
stdout
Falco sidekick
UI
Slack
S3
Serverless
Loki
User space
ring buffer
ebpf probe
Kernel module
eBPF probe
Userspace instrumentation
syscall
Drivers
Kernel

CKS exam

The Certified Kubernetes Security Specialist (CKS) program provides assurance that a CKS has the skills, knowledge, and competence on a broad range of best practices for securing container-based applications and Kubernetes platforms during build, deployment and runtime. CKA certification is required to sit for this exam.

- 2 hours
- CKA is a prerequisite
- 2 Year validity
- 2 attempts
- killer.sh/cks access
- Documentation access - Kubernetes, trivy, apparmor, falco
- $375
- Kubernetes 1.23

CKS exam focus Areas

- Cluster Setup	10% (CIS benchmark, Network policies, Ingress TLS, securing Kubernetes dashboard, verify Kubernetes binaries using checksum)
- Cluster hardening	15% (RBAC, Restrict Kubernetes API access, Service account, Kubernetes update.)
- System hardening	15% (Firewall, seccomp, Apparmor, Principle of least privilege)

CKS exam focus Areas(Continued)

- Minimize microservices Vulnerability	20%(Admission controller - Validating, mutating, PSP, OPA, security context of a pod, k8s secrets, how to use different container runtimes(gvisor,kata), mTLS
- Supply chain security	20% Imagepolicywebook, Trivy, Dockerfile best practices, Kubernetes objects best practices like run as non root etc.
- Monitoring logging and runtime security	20% (syscalls, Falco, Kubernetes Audit logs - how to enable and use, readonlyfilesystem PSP)

Tips and Tricks

- Bookmarks handy
- --dry-run flag
- Time management (when question has a lot of steps involved)
- Higher weightage first
- Take a backup of your files before making changes to kube-apiserver or falco files
- Use aliases like k=kubectl
- Be comfortable with --force while deleting
- K8s documentation navigation

Resources

- Editor.cilium.io for Network policy
- Container security and Kubernetes security books
- Kubernetes documentation
- Killer.sh CKS course
- KodeKloud CKS course
- Killercoda for CKS environment
- My CKS scenarios book
- Locally - K3s, Kind
- Cloud - managed Kubernetes like Civo, GKE

Demo