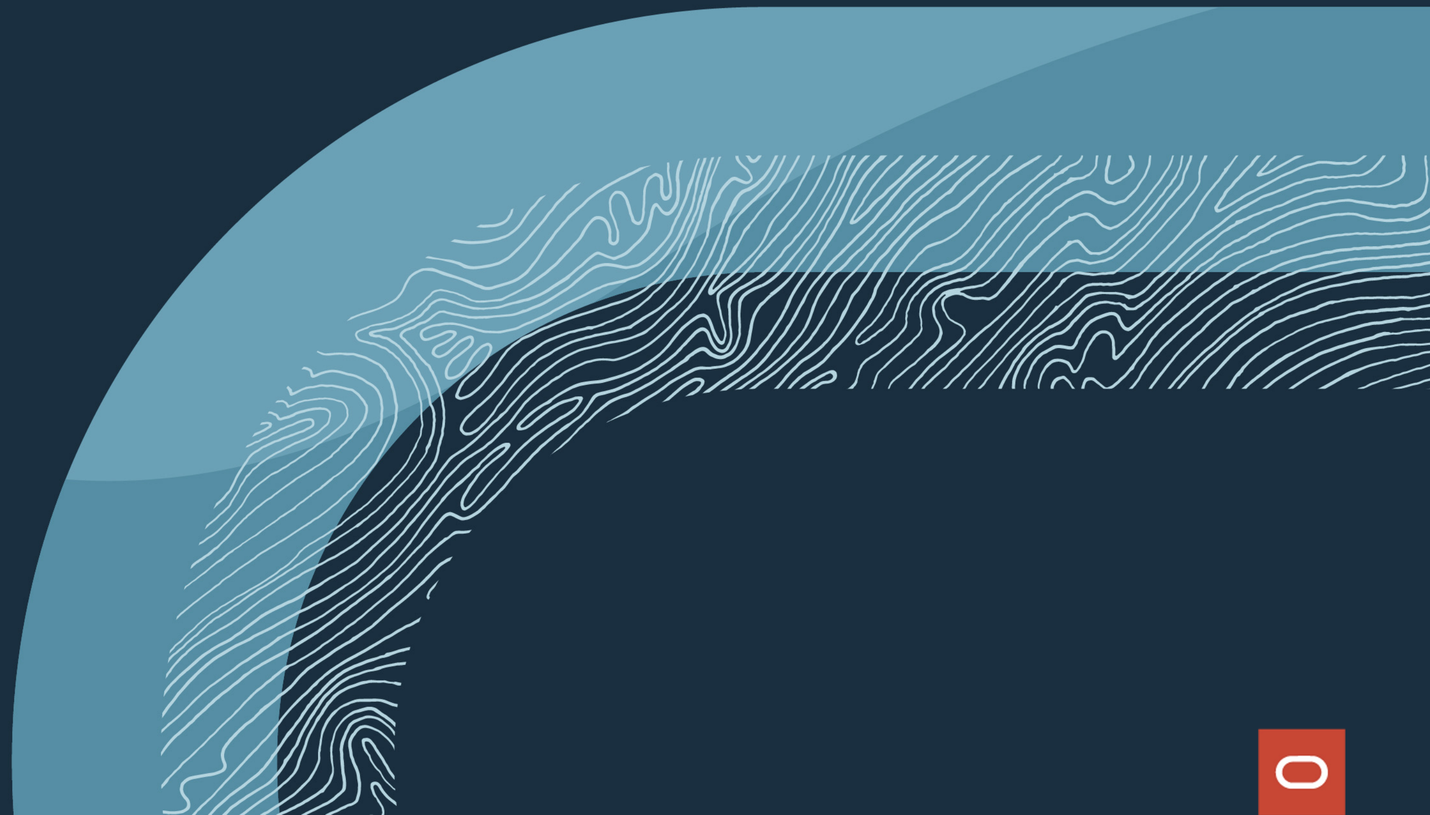
ORACLE
CloudWorld

Securing Your Managed Kubernetes With Falco

October 17–20, 2022
Caesars Forum and The Venetian
Las Vegas, NV

Challenges

Challenges on Container Security



Automation

Visibility

Consumption

Runtime Threats

Known Vulnerabilities

Human Error

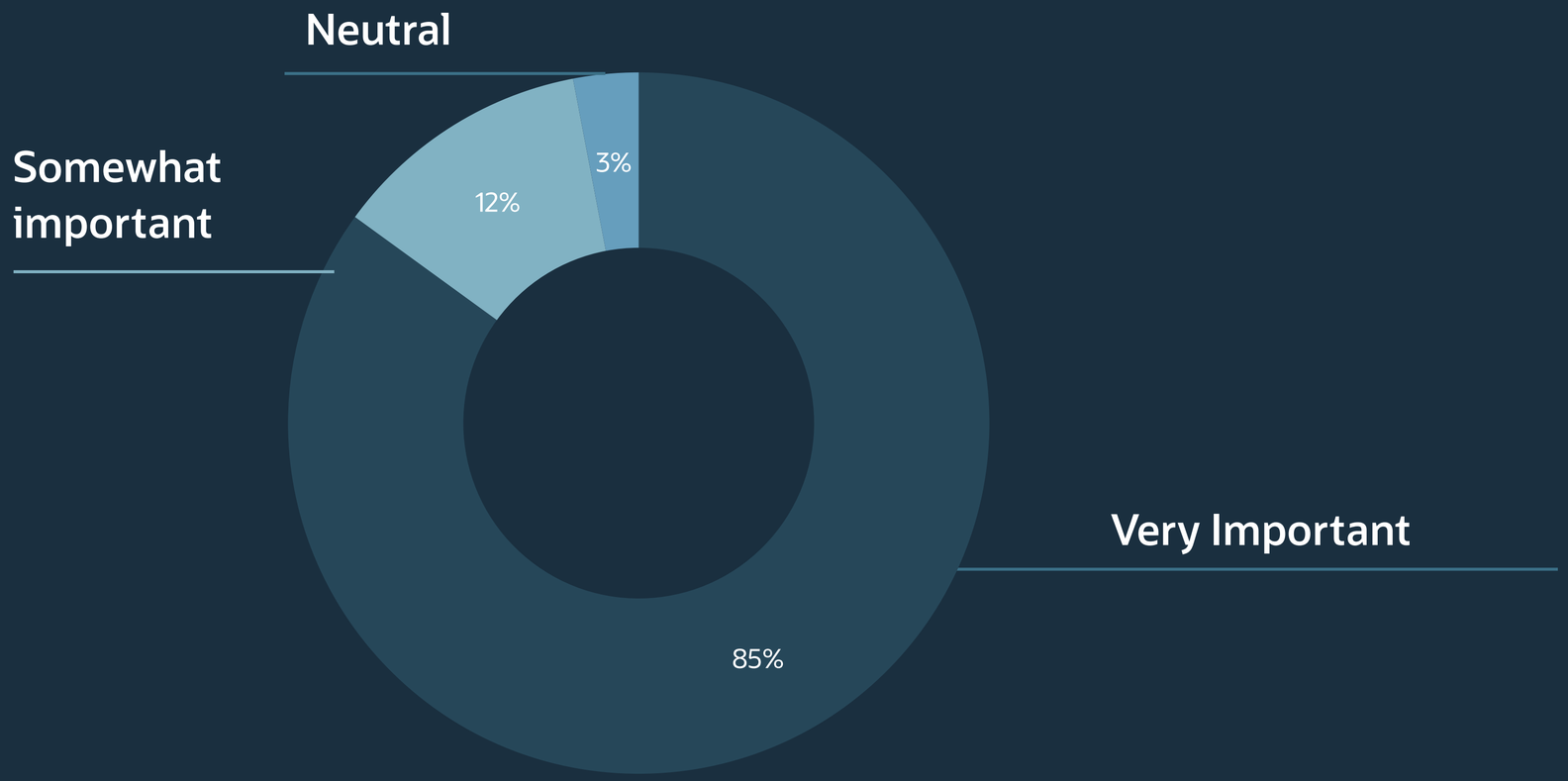
Cloud Native Security

80%

More than 80% of organizations want to build modern security systems with open source software

Source: 2021 Cloud Native Security Microsurvey

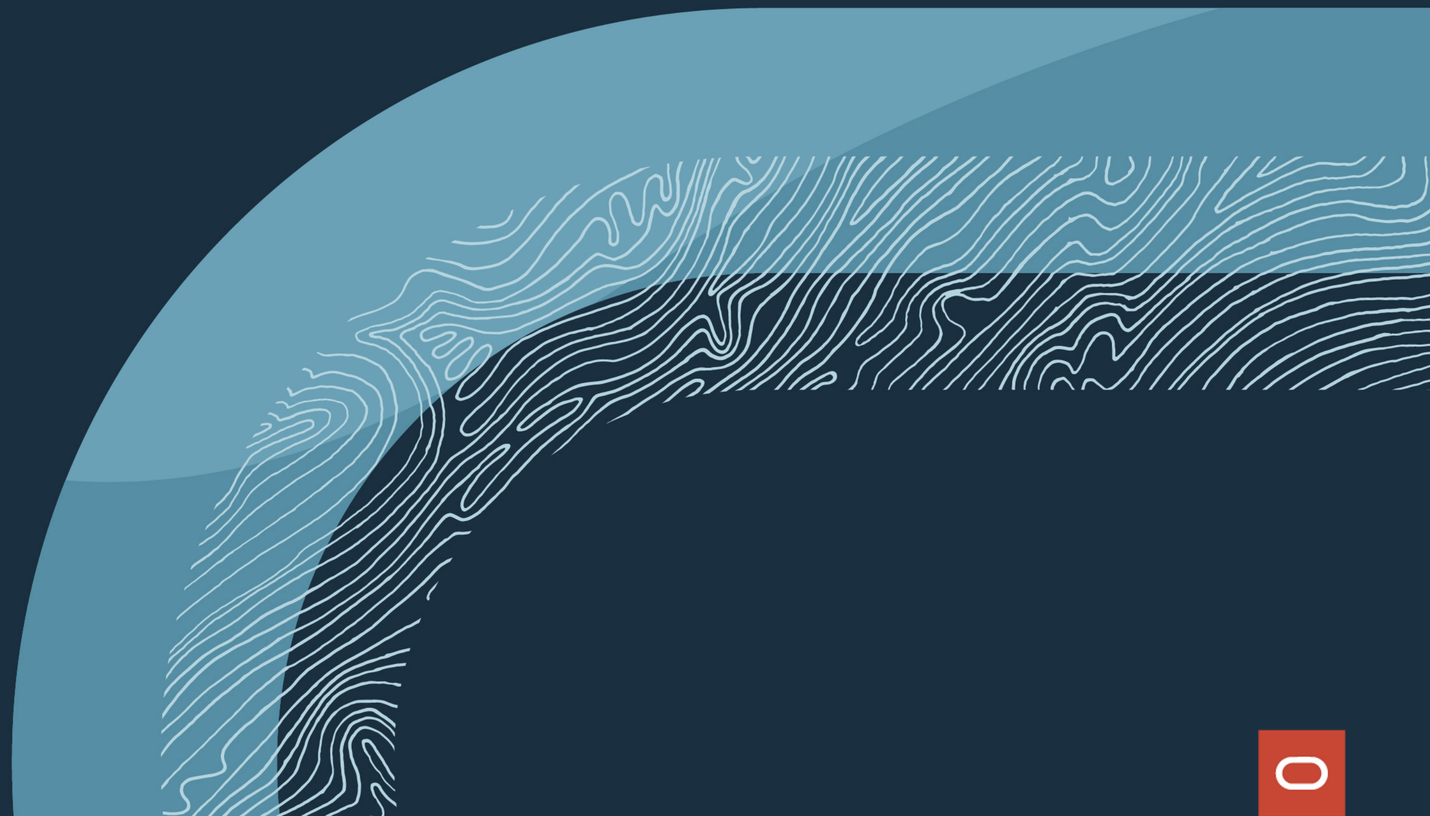
How important is modernizing security to your cloud native environment?



Source: 2021 Cloud Native Security Microsurvey

What is Falco?

Cloud-Native Runtime Security



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

A CNCF project. Falco.org

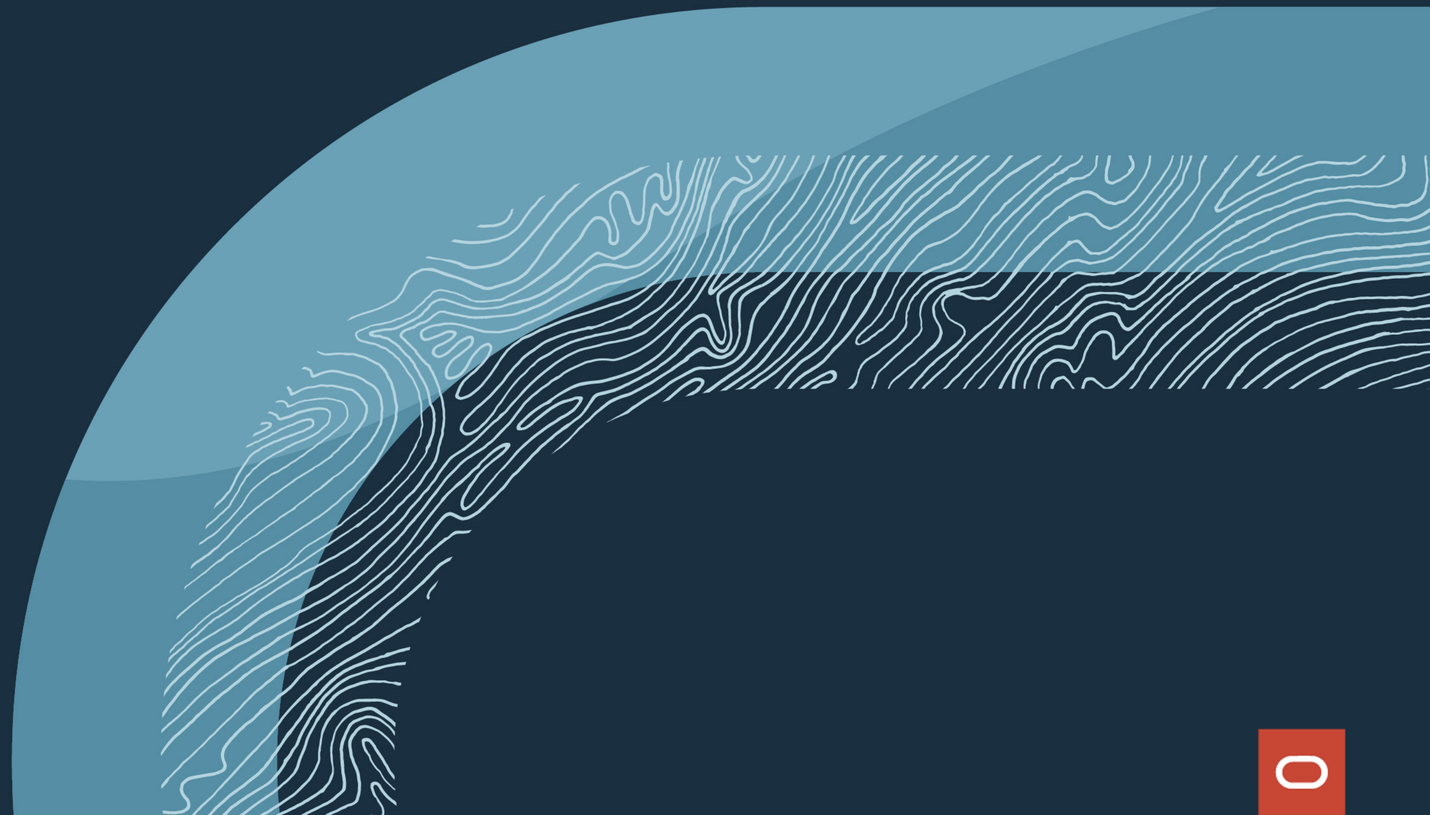
Falco Project: Cloud-Native Runtime Security

Detects threads at runtime

By observing the behavior of your applications and containers

What is OKE?

Oracle Container Engine for Kubernetes (OKE)



Oracle Container Engine for Kubernetes is an Oracle-managed container orchestration service.

https://www.oracle.com/cloud/cloud-native/container-engine-kubernetes/

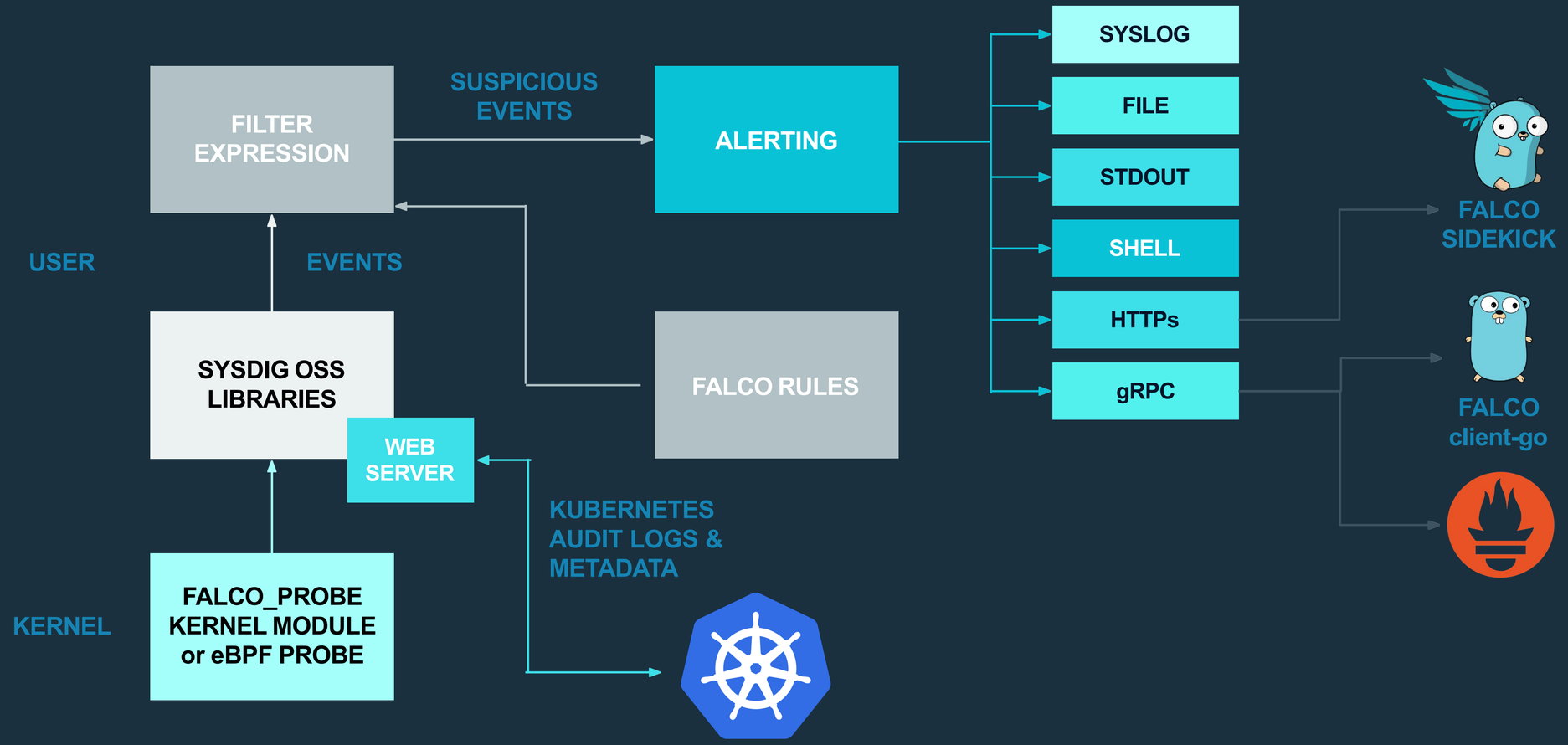
Using Falco with OKE

Watch system calls

Privilege escalation

Unexpected network connections

Falco Architecture



Audit log rule example

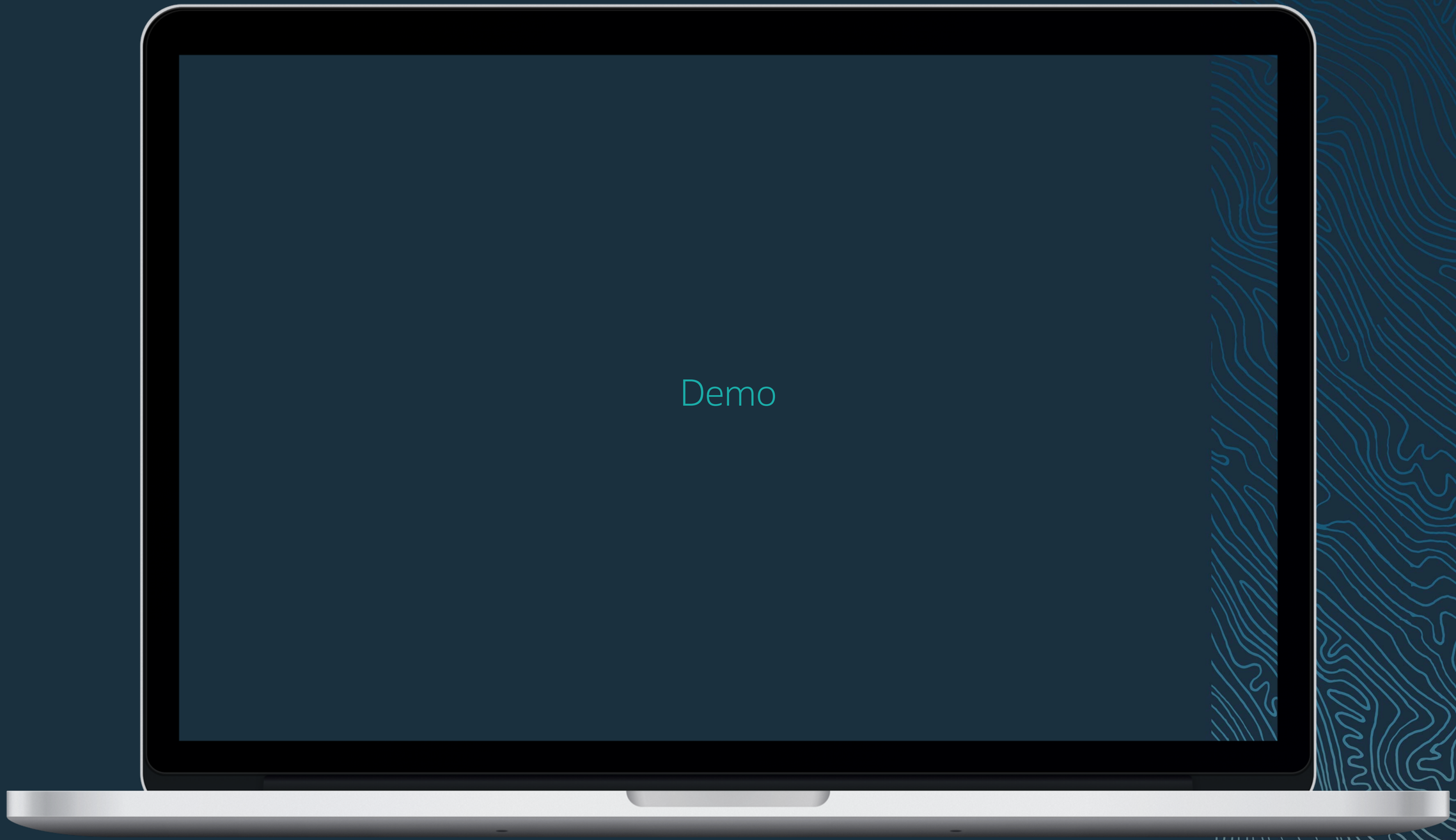
```
- macro: contains_private_credentials
condition: >
(ka.req.configmap.obj contains "user_ocid" or
ka.req.configmap.obj contains "public_ssh_key" or ka.req.configmap.obj contains “password")

- macro: configmap
condition: ka.target.resource=configmaps

- macro: modify
condition: (ka.verb in (create,update,patch))
- rule: Create/Modify Configmap With Private Credentials
desc: Detect creating/modifying a configmap containing a private credential (public ssh key, password, ..)
condition: configmap and modify and contains_private_credentials
output: K8s configmap with private credential (user=%ka.user.name
verb=%ka.verb name=%ka.req.configmap.name configmap=%ka.req.configmap.name config=%ka.req.configmap.obj)
priority: WARNING
source: k8s_audit
tags: [k8s]
```

Example of a Falco Rule on OKE

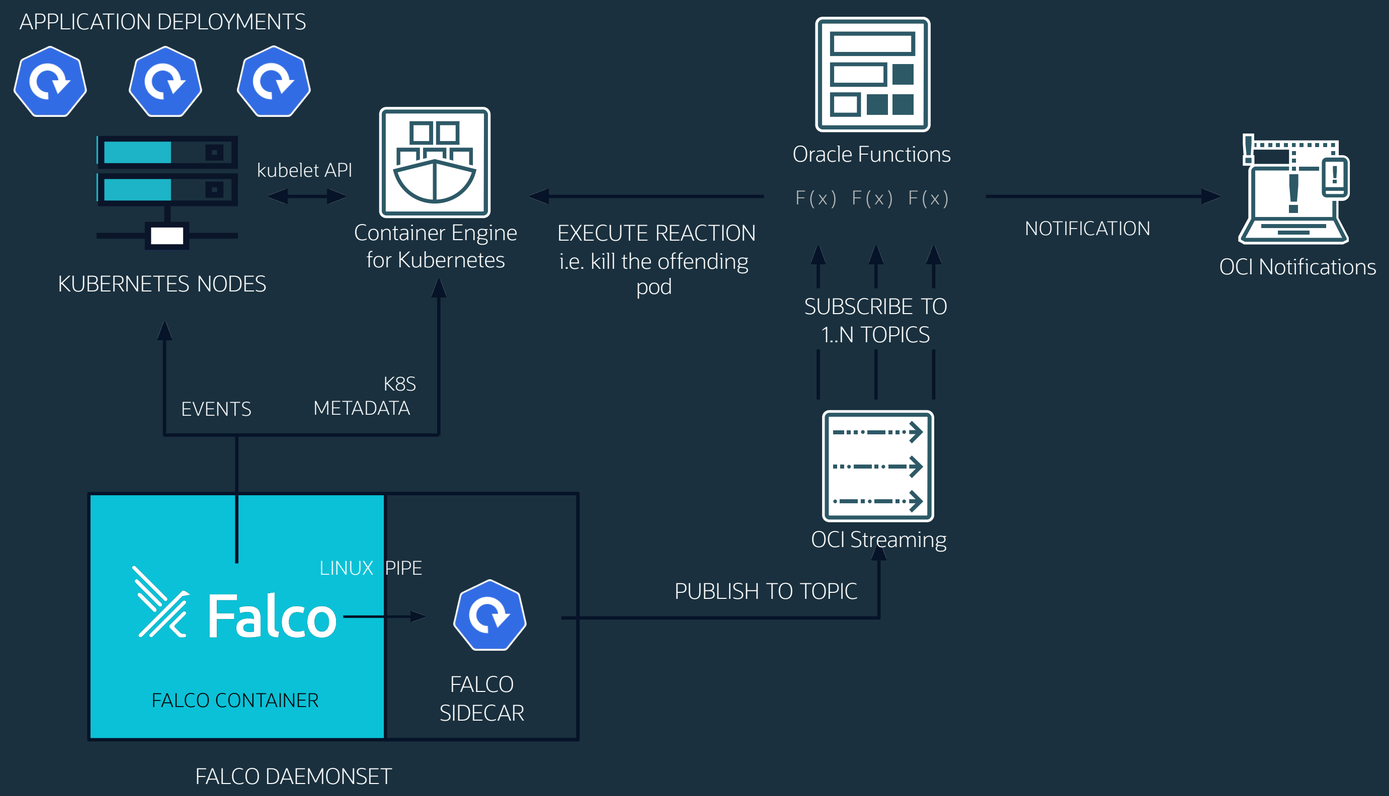
```
- macro: kube_apiserver_consider_syscalls
condition: (evt.num < 0)

- macro: app_kube_apiserver
condition: container and container.image contains "kube-apiserver"

- list: kube_apiserver_allowed_inbound_ports_tcp
items: [6443]

- rule: Unexpected inbound tcp connection kube_apiserver
desc: Detect inbound traffic to kube_apiserver using tcp on a port outside of expected set
condition: inbound and evt.rawres >= 0 and not fd.sport in (kube_apiserver_allowed_inbound_ports_tcp) and
app_kube_apiserver
output: Inbound network connection to kube_apiserver on unexpected port (command=%proc.cmdline
pid=%proc.pid connection=%fd.name sport=%fd.sport user=%user.name %container.info image=%container.image)
priority: NOTICE

- list: kube_apiserver_allowed_processes
items: ["kube-apiserver"]
```

Example of a Falco Rule on OKE

```
- rule: Unexpected spawned process kube_apiserver
desc: Detect a process started in a kube_apiserver container outside of an expected set
condition: spawned_process and not proc.name in (kube_apiserver_allowed_processes) and app_kube_apiserver
output: Unexpected process spawned in kube_apiserver container (command=%proc.cmdline pid=%proc.pid
user=%user.name %container.info image=%container.image)
priority: NOTICE

- list: kube_apiserver_allowed_syscalls
items: [accept, connect, socket]

- rule: Unexpected syscall kube_apiserver
desc: Detect a syscall in a kube_apiserver container outside of an expected set
condition: kube_apiserver_consider_syscalls and not evt.type in ("<unknown>",
kube_apiserver_allowed_syscalls) and app_kube_apiserver
output: Unexpected syscall in kube_apiserver container (command=%proc.cmdline pid=%proc.pid
user=%user.name syscall=%evt.type args=%evt.args %container.info image=%container.image)
priority: NOTICE
warn_evttypes: False
```



Security Orchestration with Falco, OKE and other OCI Services



References:

Falco Website:

- https://falco.org

Falco GitHub:

- https://github.com/falcosecurity/falco

Falco Documentation:

- https://falco.org/docs

Falco 0.33.0 a.k.a. "the pumpkin release 🎃" released today:

- https://falco.org/blog/falco-0-33-0/

Incredible Resources:

For Developers, by Developers

Join us for tons of technical content & community

Join us on Slack!

Follow along for troubleshooting, community, and pictures of pets

Check out developer.oracle.com

Your one stop hub to overload on technical content

Follow Along.
Get Involved.
Grab Some Swag!

Check out our social channels for all the latest with Oracle Developer!

Check us out

@OracleDevs

@thelumins

Use the hashtag to get some swag!

#ODevRel

#DevNucleus

#BeatMaxV

Posted on social and tagged us? You deserve a treat - come find us at the Swag Tower at the DevNucleus!

You Don’t Want to Miss!

Anytime

#BeatMaxV on the Red Bull Racing Playseats. Highest scores on the leaderboard gets some great prizes!

October 18th | 4-5pm

Mark your calendars for the Developer Keynote! Hear from MosaicML, Java and a Sports Panel with Red Bull Racing and SailGP

October 19th | 4:30pm

Join Oracle and MosaicML for the Happy Hour Celebration! Come to DevNucleus for drinks, networking, and tons of fun

Anytime

Don’t miss out on your chance to take a selfie with Devy at the #DevNucleus selfie station

ORACLE
CloudWorld

Thank you

“Security planning is never too much.”

Adao Oliveira Junior, Cloud Solutions Architect
adao.junior@oracle.com