MAINTAINER TRACK, FALCO

No Fear, Falco Is Looking After Us!

Carlos Panato, Chainguard
Hendrik Brückner, IBM
Melissa Kilby, Apple
Jason Dellaluce, Sysdig
Luca Guerra, Sysdig

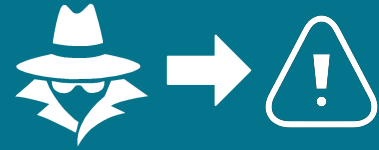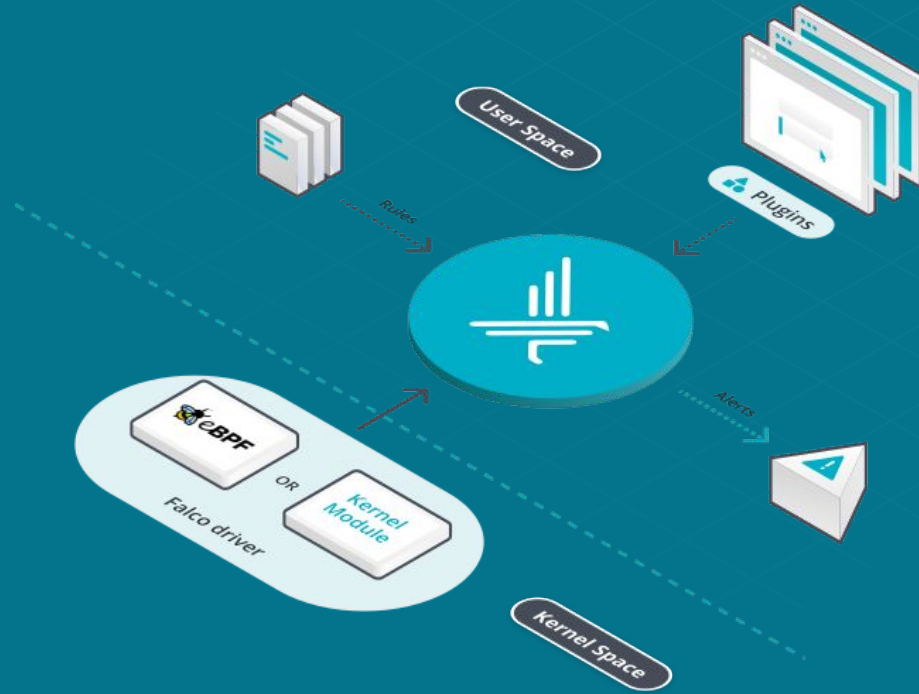**Wednesday April 19 | 16:30 - 17:05 CEST | Forum Center, E103-104**
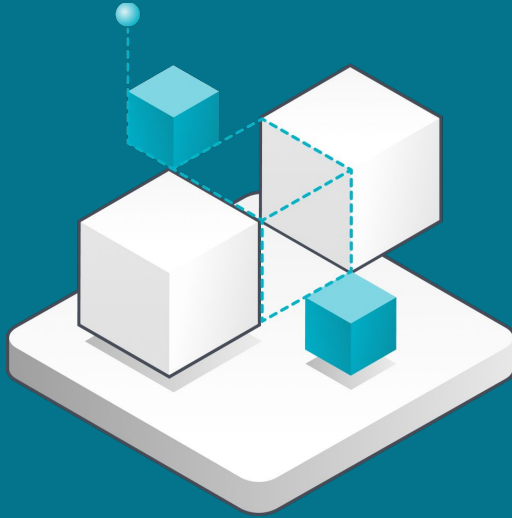
KubeCon | CloudNativeCon

Europe 2023

What is Falco and its purpose?

How do you spend your time and balance priorities?
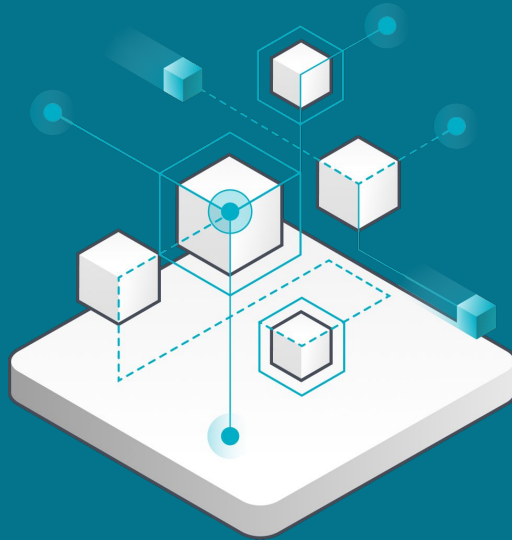
Falco's new project roadmap and governance

Tell us about your experience as a Falco maintainer?

Falco's own security

What is the most impactful thing you have learned since becoming a maintainer?

Dynamic system call selection mechanisms

How can others get involved?

Welcome to the Falco flock!

Falco is an open source security project, hosted by the CNCF. Our community is passionate about securing containers and clouds. We love open source and Falco. As a vendor neutral project, **we** welcome a broad range of contributions. Please take a moment to check out the different ways you can participate or obtain support. Come fly with us!

Contribute

Connect

Follow us on social

🐦 Twitter   in Linkedin

Join Kubernetes #falco

Slack

Understand our governance

Github

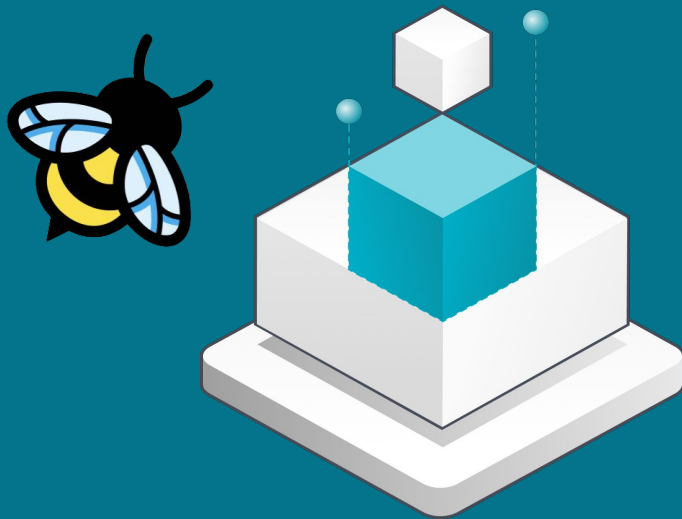## Create an issue

Meet our maintainers

What are the benefits to your organization from the perspective of a maintainer?

Falco's modern eBPF kernel driver

Falco is up and running, what happens on Day 2?
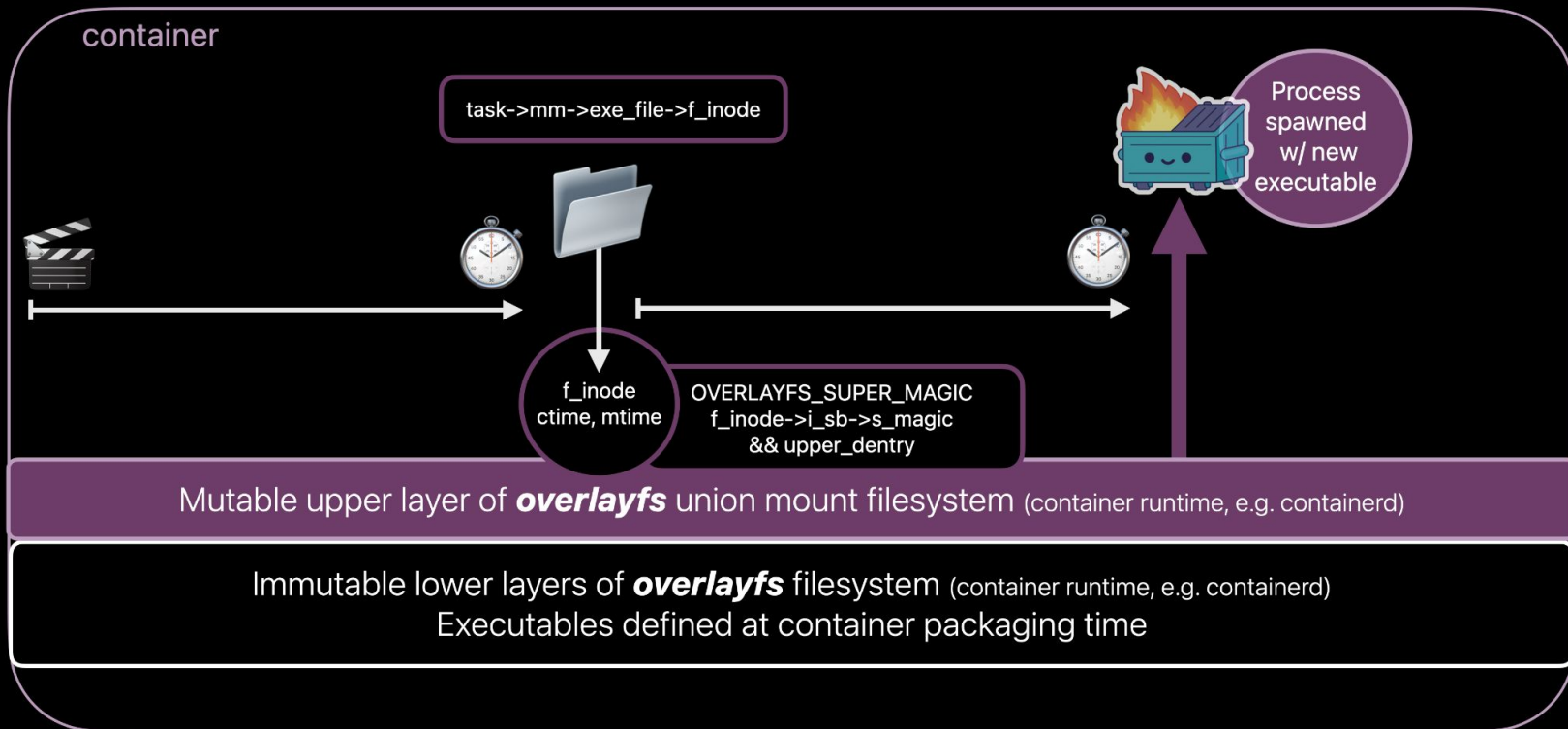
Resource Utilization Metrics

Performance

Scale

Insights

Threat Detection Capabilities

What are recent wins to catch more bad stuff?

Drop and execute new executable in container

container

task->mm->exe_file->f_inode

Process spawned w/ new executable

f_inode
ctime, mtime

OVERLAYFS_SUPER_MAGIC
f_inode->i_sb->s_magic
&& upper_dentry

Mutable upper layer of **overlayfs** union mount filesystem (container runtime, e.g. containerd)

Immutable lower layers of **overlayfs** filesystem (container runtime, e.g. containerd)
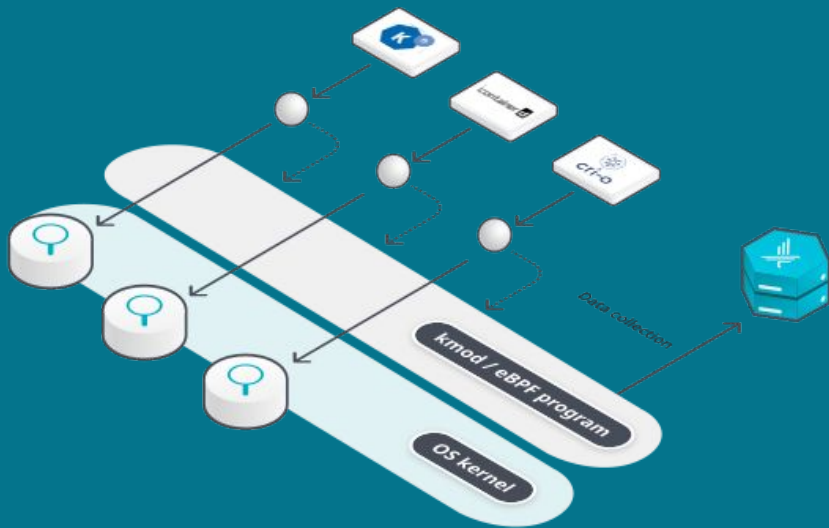Executables defined at container packaging time

What are recent wins to make it easier to use Falco?

Plugins and Rules deployment workflows
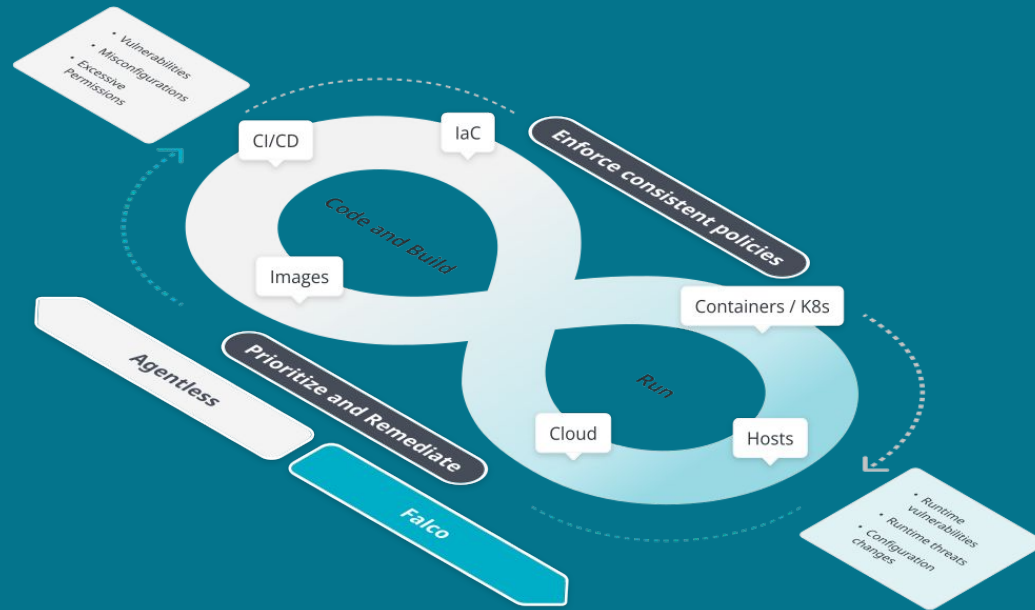
How do we test Falco?

New e2e and unit testing frameworks

How does Falco integrate with other CNCF projects?

What is next in Falco?

Join the Falco community ♡

Thank you