Detecting Security Policies Violation Using Falco: a Practical Introduction

Leonardo Grasso

Falco

In this talk...

Intro to Falco

Demo “create a custom rule”

Me having fun with ASCII art 😱

A bit of history...

Jan 2016
First commit

Oct 2018
Donated to CNCF

Dec 2019
Promoted to Incubation

About me

Leonardo Grasso

leogr

Open Source Software Engineer
@Sysdig

Falco Maintainer
@falcosecurity

github.com/leogr

twitter.com/leogrease

Falco

cloud native runtime security

What is Falco?

Kernel Events as source of truth

Enriched with metadata

Assert against rules at runtime

Alert during violation events

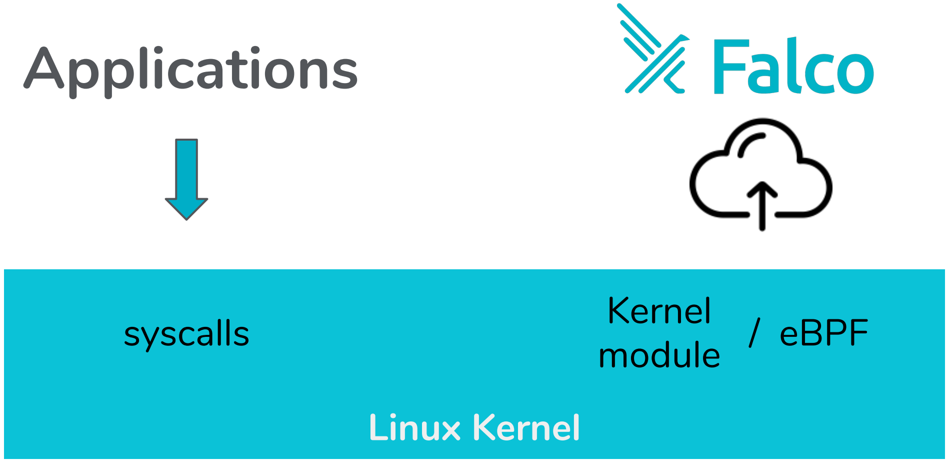
Why Falco?

Unexpected change in system

Runtime based detection

Enabling prevention, too

How it works



Applications

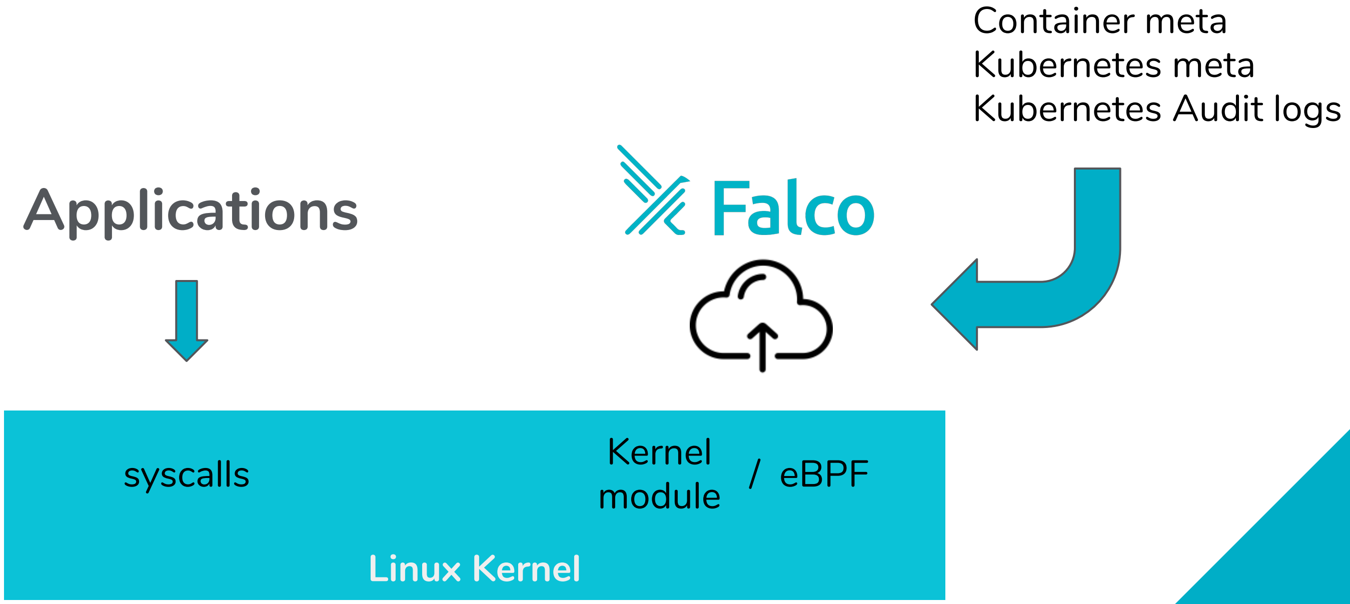
Falco

syscalls

Kernel module / eBPF

Linux Kernel

How it works



Container meta
Kubernetes meta
Kubernetes Audit logs

Applications

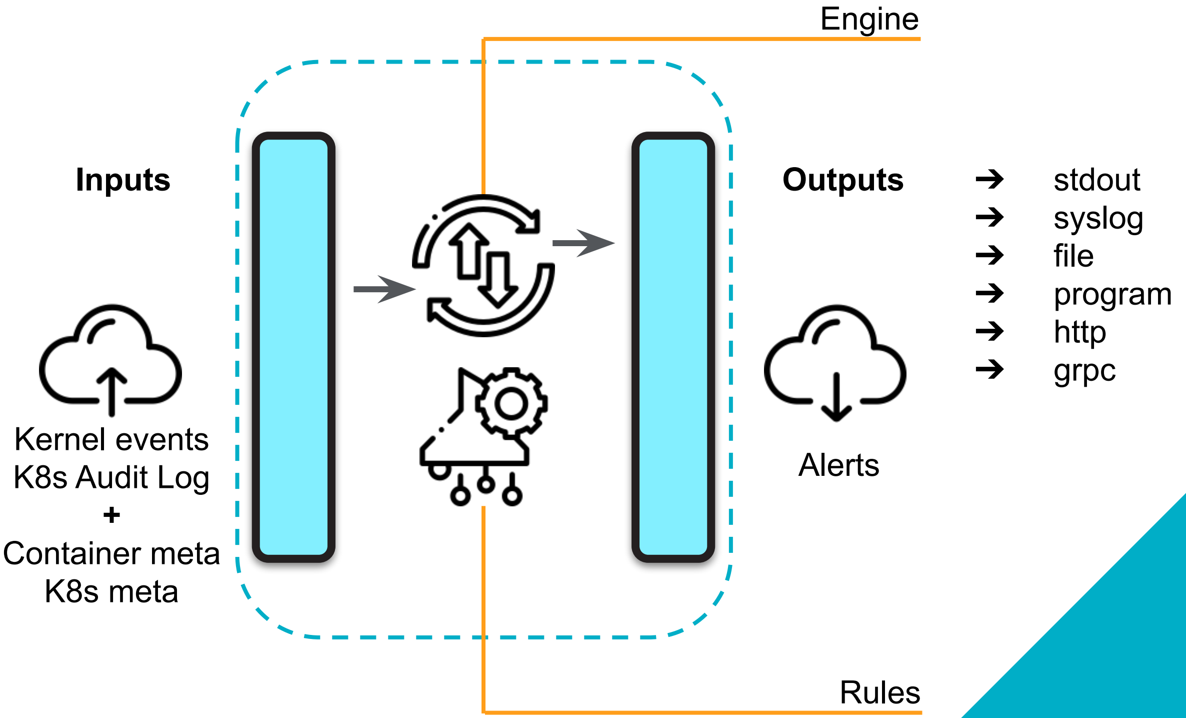
Falco

syscalls

Kernel module / eBPF

Linux Kernel

How it works



Engine

Inputs

Kernel events
K8s Audit Log
+
Container meta
K8s meta

Outputs

Alerts

→ stdout
→ syslog
→ file
→ program
→ http
→ grpc

Rules

The rules

A rule defines the **conditions** and the **message**.

Rule examples

A shell is run in a container	container.id != host and proc.name = bash
Write below binary dir	open_write and fd.directory in (/bin, /sbin, /usr/bin, /usr/sbin)
Container namespace change	evt.type = setns and not proc.name in (docker, sysdig)
Non-device files written in /dev	(evt.type = create or evt.arg.flags contains O_CREAT) and proc.name != blkid and fd.directory = /dev and fd.name != /dev/null

Demo

Create a custom rule.

Resources

falco.org

github.com/falcosecurity

Other projects

github.com/falcosecurity/pdig

github.com/falcosecurity/falcosidekick

github.com/falcosecurity/falco-exporter

Join our community!

#falco channel on the Kubernetes Slack

More details 👉 github.com/falcosecurity/community

Leonardo Grasso

github.com/leogr

Thank you!