




Security In the Cloud With Falco: Overview And Project Updates

✓ **feat(falco): maintainers track**

[Browse files](#)

Signed-off-by: Jason Dellaluce <jasondellaluce@gmail.com>

Signed-off-by: Luca Guerra <luca@guerra.sh>

 **kubecon-cnc-na** (#2022)

 **0.33.0** ...



2 people authored and **poiana** committed on Oct 28



About us



Jason Dellaluce
Open Source Engineer
Falco Core Maintainer


jasondellaluce 

jasondellaluce 



Luca Guerra
Open Source Engineer
Falco Core Maintainer

 LucaGuerra

 lucklypse



What is Falco?



A security camera detecting unexpected behavior, intrusions, and data theft in real time

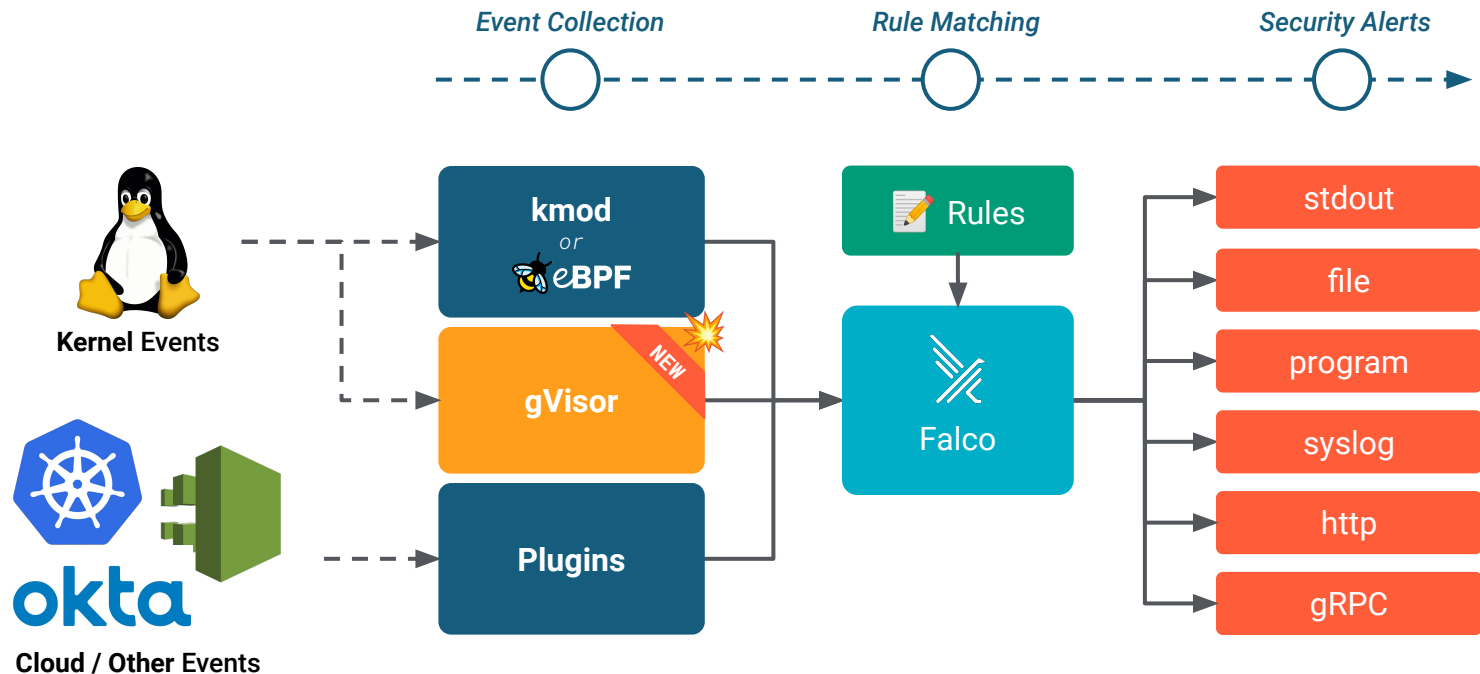


The cloud-native runtime
security project

The de facto Kubernetes
threat detection engine



How does Falco work?



What's New in Falco

Lots of exciting stuff 🚀



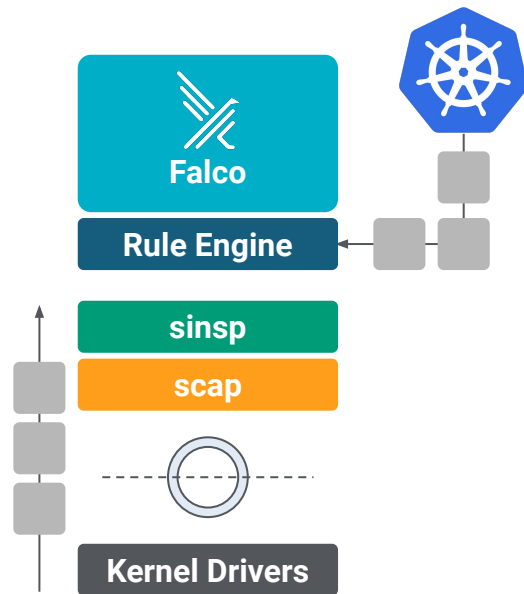
Official ARM64 Support

- ✓ v0.32+ officially supports ARM64!
- ✓ Artifacts and container images for both AMD64 and ARM64
- ✓ Plugins built for ARM64 too 😊
- ✓ Kernel module and eBPF probes now pre-built for both platforms



Event Sources: Before Falco 0.31

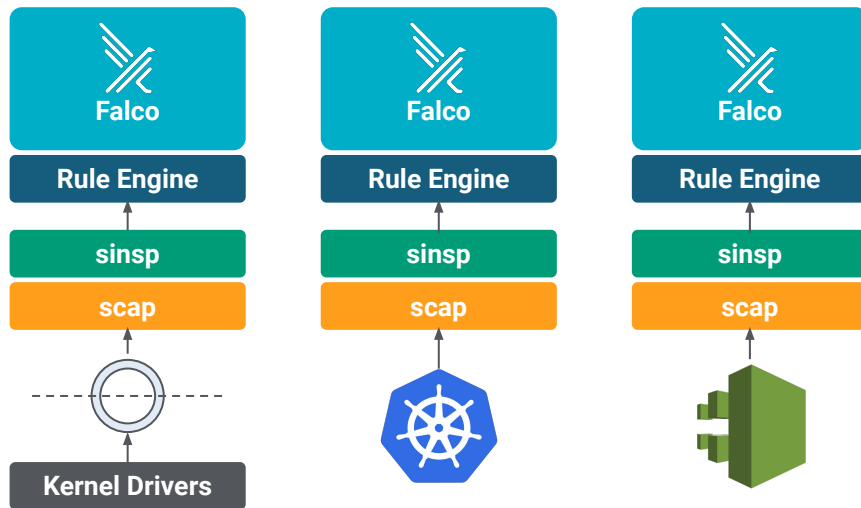
- No real notion of “*event source*”
- Falco designed for **kernel events**
- Basic support for **k8s audit events**
 - Hacked into the Falco application
- **Syscalls and k8s audit events together**
 - Ambiguous deployment requirements
 - No real parallelization safety guarantees





Event Sources: After Falco 0.31

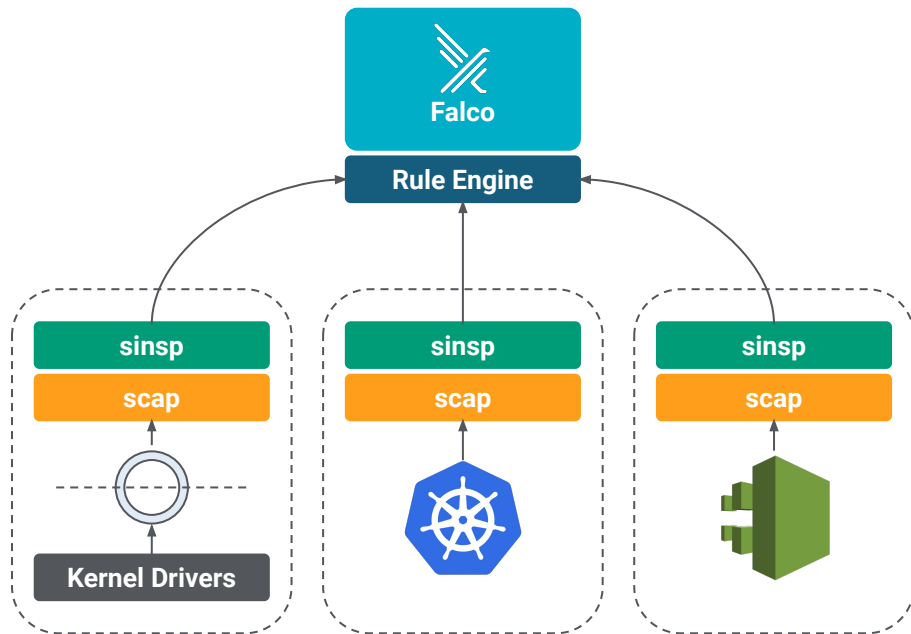
- Standard plugin system
- Notion of “event source”
 - `syscall`, `aws_cloudtrail`, `k8s_audit`, ...
- K8s audit events re-written as a plugin in v0.32 (in Go 🍷)
- Events from only one source
- Many sources → Many Falcos





Event Sources: After Falco 0.33

- Multiple simultaneous event sources with safe thread isolation
- Feature and performance parity with multiple one-sourced Falcos
- Opportunity for new use cases
- See 📖 falcosecurity/falco#2074

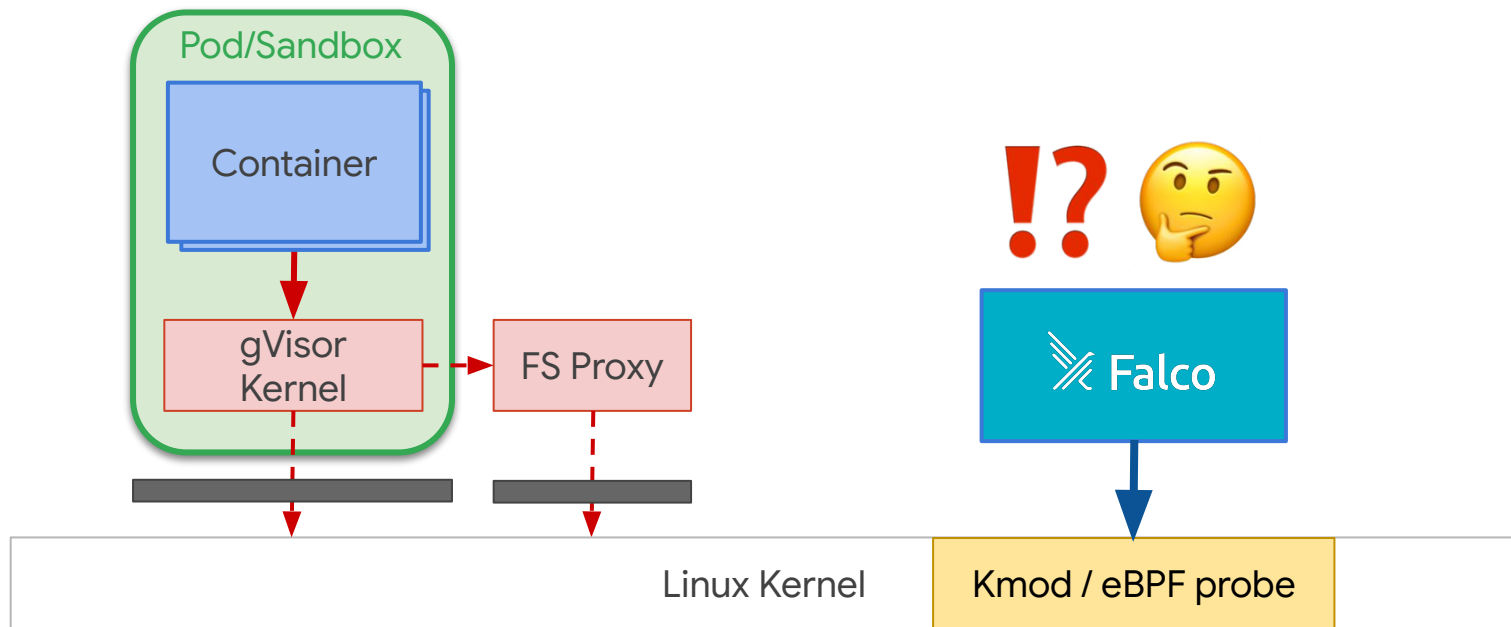




gVisor - what is it?

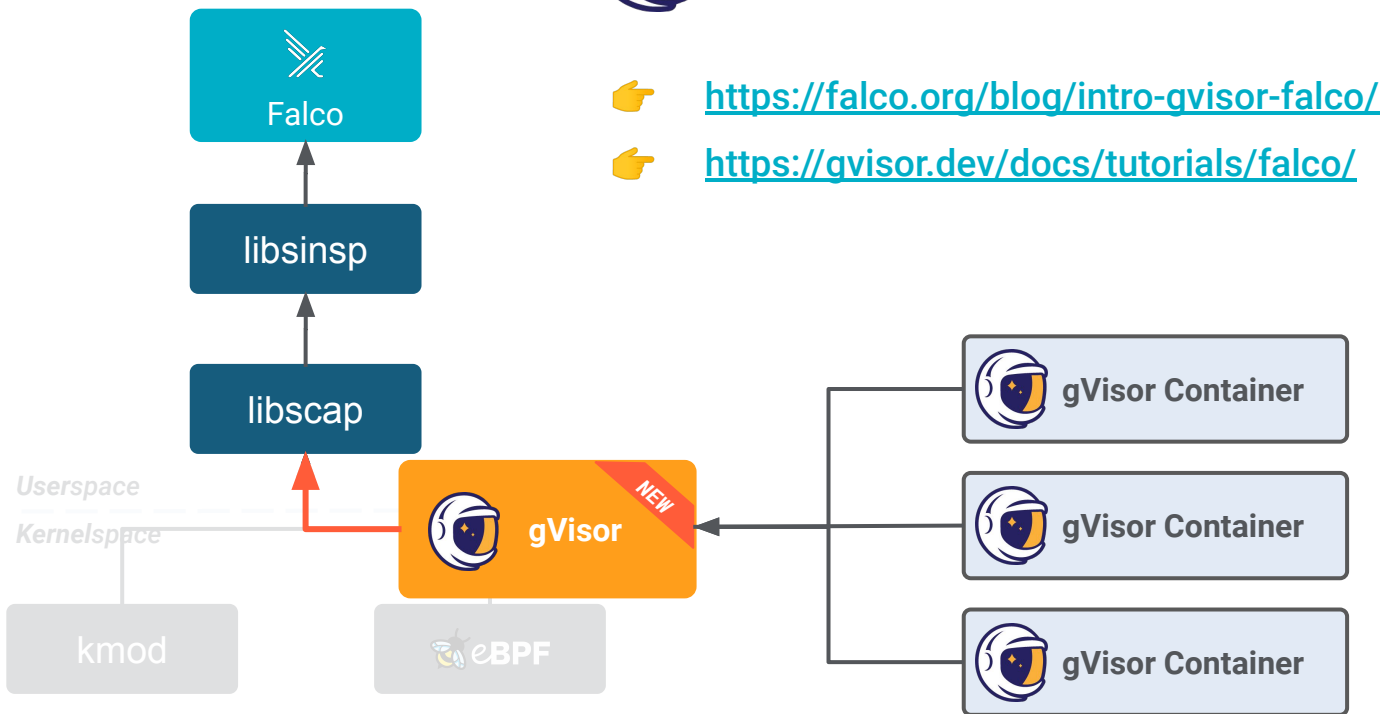


OSS Sandboxing Technology from Google, used in AppEngine, GKE/GCP ...





gVisor support



<https://falco.org/blog/intro-gvisor-falco/>



<https://gvisor.dev/docs/tutorials/falco/>

Security Rules



- rule: **Directory traversal monitored file read**

desc: >

Web applications can be vulnerable to directory traversal attacks that allow accessing files outside of the web app's root directory (e.g. Arbitrary File Read bugs).

System directories like /etc are typically accessed via absolute paths. Access patterns outside of this (here path traversal) can be regarded as suspicious.

This rule includes failed file open attempts.



- rule: **Read environment variable from /proc files**

desc: An attempt to read process environment variables from /proc files

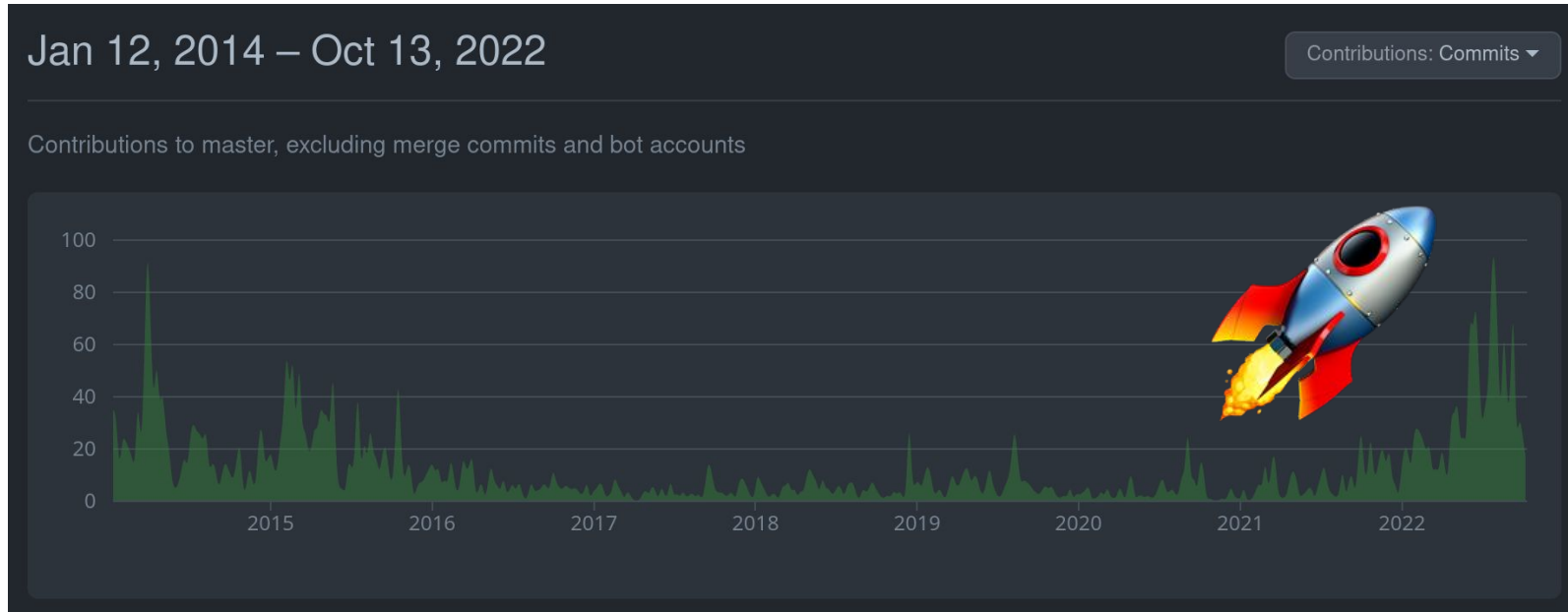
- Vulnerability Rules Updates:
 - 🔑 CVE-2021-44228 (log4Shell)
 - 🔑 CVE-2019-5736
- Rules refactor and cleanup

Falco Libraries

What makes Falco tick 



Most contributions ever!





An inspirational quote

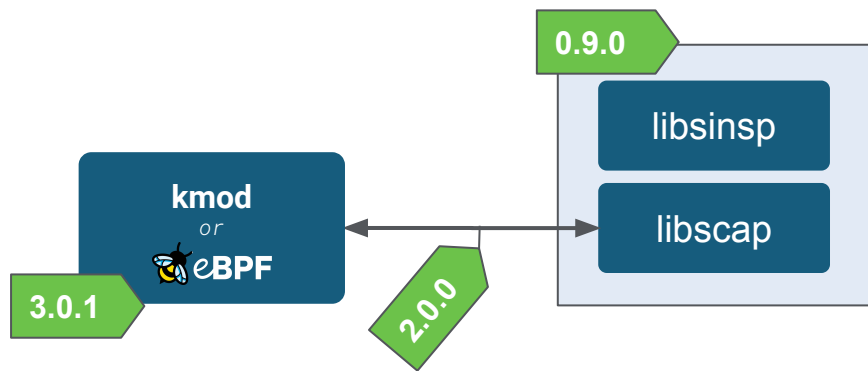
Every time we pull from you folks, we get some “surprises”

– A downstream contributor



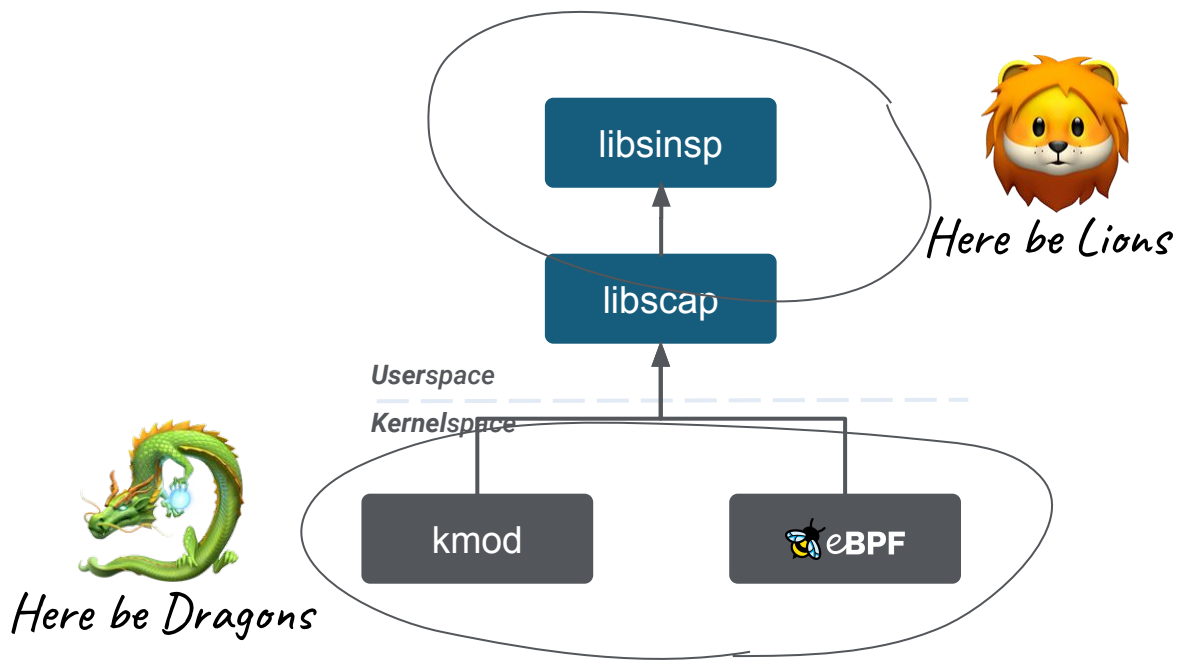
Libraries and Driver versioning

- Versions for everything!
- <https://github.com/falcosecurity/libs/blob/master/driver/README.VERSION.md>



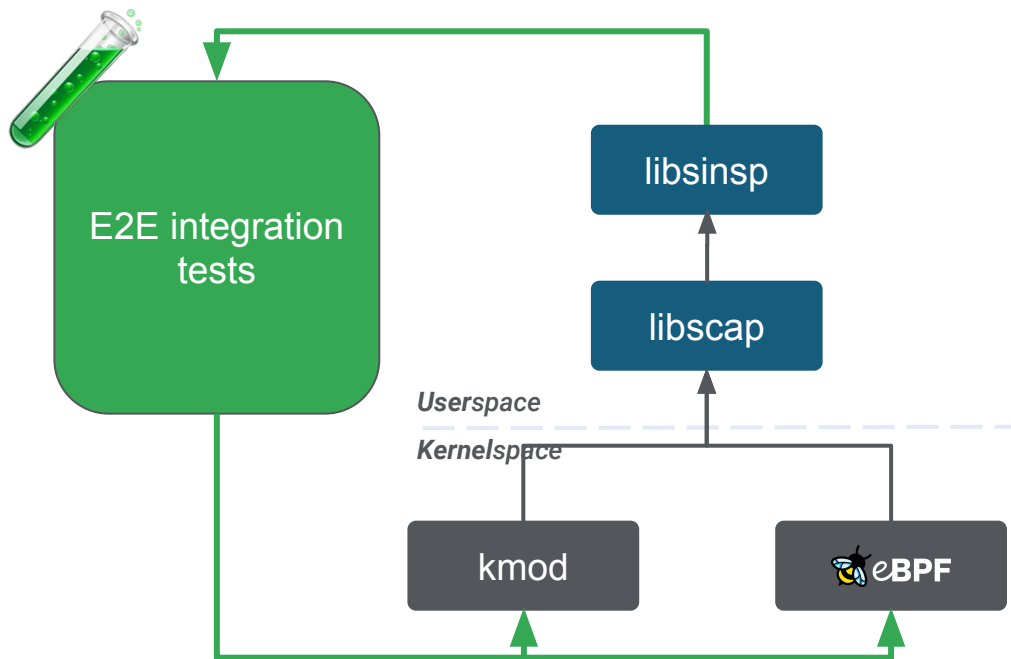


Testing Improvements





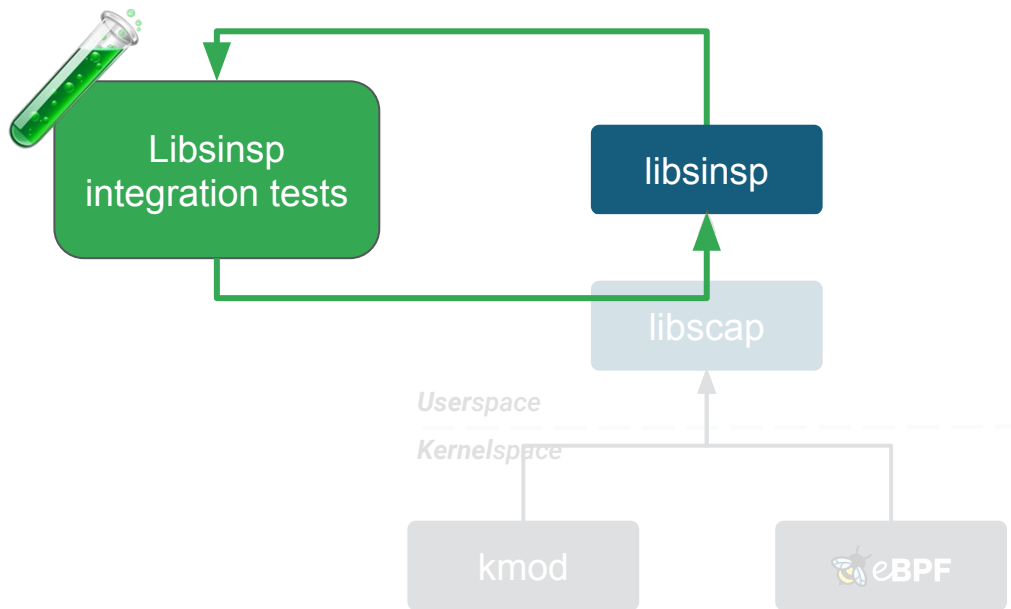
Testing improvements - end to end



- ✓ Realistic
- ✓ Common Syscalls
- ✓ Easily add multiple architectures



Testing improvements - libinsp



- ✓ Fast to run
- ✓ Test corner cases
- ✓ ASan support included!



Selective Captures

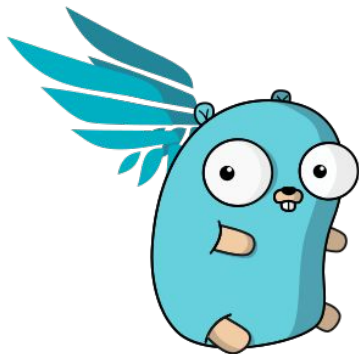
- Tracing all syscalls can be cumbersome for some clients that have deep knowledge of what they need
- Clients can now specify exactly what they need
- Several community clients requested that!
- Clients need to be careful not to break compatibility with the `sinsp` functions that they require

Ecosystem

Falco does not fly alone



Falcosidekick



ARM support



Policy Reports



Cosign



New integrations

Syslog




AWS Kinesis



Zoho Cliq



Falcosidekick UI v2.0.2

 Falcosidekick UI

Total 93504 Critical 4227 Debug 1842 Error 11244 Informational 17389 Notice 25623 Warning 33179

DASHBOARD EVENTS INFO

Sources Priorities Rules Tags Since

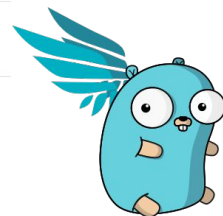
Error Informational

1h

Search

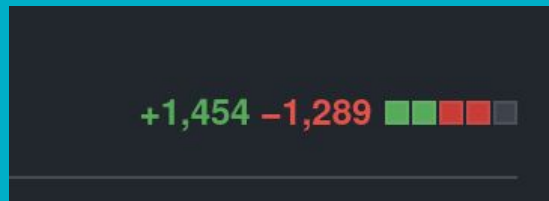
Total 244 Error 96 Informational 148

Timestamp	Source	Priority	Rule	Output	Tags
2022/05/11 12:17:53.550	k8s_audit	Informational	K8s Deployment Deleted	K8s Deployment Deleted (user=%ka.user.name deployment=%ka.target.name ns=%ka.target.namespace resp=%ka.response.code decision=%ka.auth.decision reason=%ka.auth.reason) ka.auth.decision %ka.auth.decision ka.auth.reason %ka.auth.reason ka.response.code %ka.response.code ka.target.name %ka.target.name ka.target.namespace %ka.target.namespace ka.user.name %ka.user.name	k8s
2022/05/11 12:17:38.536	syscalls	Informational	System user interactive	System user ran an interactive command (user=%user.name user_loginuid=%user.loginuid command=%proc.cmdline container_id=%container.id image=%container.image.repository) container.id %container.id container.image.repository %container.image.repository proc.cmdline %proc.cmdline user.loginuid %user.loginuid user.name %user.name	users mitre_remote_access_tools
2022/05/11 12:17:29.527	syscalls	Error	Write below rpm database	Rpm database opened for writing by a non-rpm program (command=%proc.cmdline file=%fd.name parent=%proc.pname pcmdline=%proc.pcmdline container_id=%container.id image=%container.image.repository) container.id %container.id container.image.repository %container.image.repository fd.name %fd.name proc.cmdline %proc.cmdline proc.pcmdline %proc.pcmdline proc.pname %proc.pname	filesystem software_mgmt mitre_persistence
2022/05/11 12:17:07.518	syscalls	Informational	Container Run as Root User	Container launched with root user privilege (uid=%user.uid container_id=%container.id container_name=%container.name image=%container.image.repository.%container.image.tag) container.id %container.id container.image.repository %container.image.repository container.image.tag %container.image.tag container.name %container.name k8s.ns.name %k8s.ns.name k8s.pod.name %k8s.pod.name user.uid %user.uid	container process
2022/05/11 12:16:52.511	k8s_audit	Informational	K8s Role/Clusterrolebinding Created	K8s Cluster Role Binding Created (user=%ka.user.name binding=%ka.target.name subjects=%ka.req.binding.subjects role=%ka.req.binding.role resp=%ka.response.code decision=%ka.auth.decision reason=%ka.auth.reason) ka.auth.decision %ka.auth.decision ka.auth.reason %ka.auth.reason ka.req.binding %ka.req.binding ka.response.code %ka.response.code	k8s





New Helm chart



- ✓ Plugin Support
- ✓ Modernized
- ✓ Simplified user experience
- ✓ Supports kmod/eBPF/plugins with or without init containers



Kernel Crawler: a New Tool

- Scrapes the web and generates driverkit configs
- Pre-built eBPF probes and kmodes for the most up-to-date kernels
- Build matrix is growing fast and automatically 🤖
- Scraped info open database 📍 falcosecurity.github.io/kernel-crawler
- List of all prebuilt drivers 📍

download.falco.org/driver/site/index.html



Crawler



Driverkit



download.falco.org

driver-loader



Falco



Kernel Crawler: Sneak Peek

Lib:

Arch:

Kind:

Target:

Show entries

Search:

Lib	Arch	Target	Kind	Kernel	Name	Size	Download	LastModified	Link
3.0.1+driver	x86_64	amazonlinux2	ebpf	4.14.101-91.76.amzn2.x86	falco_amazonlinux2_4.14.101-91.76.amzn2.x86_64_1.o	4.1 MB	↓	2022-10-19T07:34:03.000Z	↗
3.0.1+driver	x86_64	amazonlinux2	ebpf	4.14.104-95.84.amzn2.x86	falco_amazonlinux2_4.14.104-95.84.amzn2.x86_64_1.o	4.1 MB	↓	2022-10-19T08:10:35.000Z	↗
3.0.1+driver	x86_64	amazonlinux2	ebpf	4.14.106-97.85.amzn2.x86	falco_amazonlinux2_4.14.106-97.85.amzn2.x86_64_1.o	4.1 MB	↓	2022-10-19T08:26:07.000Z	↗

Plugin Updates

PORTED!



Kubernetes
Audit Logs

NEW!



AWS EKS

NEW!



GitHub

IMPROVED!



AWS Cloudtrail

IMPROVED!




(remember that
Uber MFA attack?)











- **Plugin SDK Go** – New features, better performance, Go plugin loader
- **Plugin SDK C++** – In the making, will be released as stable shortly



Governance Improvements

- Governance has been reviewed
- Most relevant clear-ups:
 - Roles of community members
 - Leadership and decision making
 - Escalation paths, conflict resolution, lazy consensus 🚀
- Formally recognized *Emeritus Maintainers*
- Take a look 🙌 [GOVERNANCE.md](#)

 leogr docs(GOVERNANCE.md): improve sentence clarity ...

          11 contributors

313 lines (200 sloc) | 21.9 KB

The Falco Project Governance

This document describes the fundamental principles The Falco Project adheres to, extension and modification.

Table of Contents

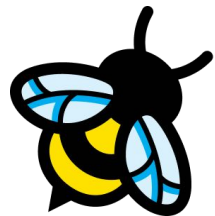
- [Principles](#)
- [Project Evolution](#)
- [Repositories](#)
 - [Core repositories](#)
 - [Repository ownership](#)
- [Community](#)
 - [Adopters](#)

Upcoming

The even fresher stuff



eBPF

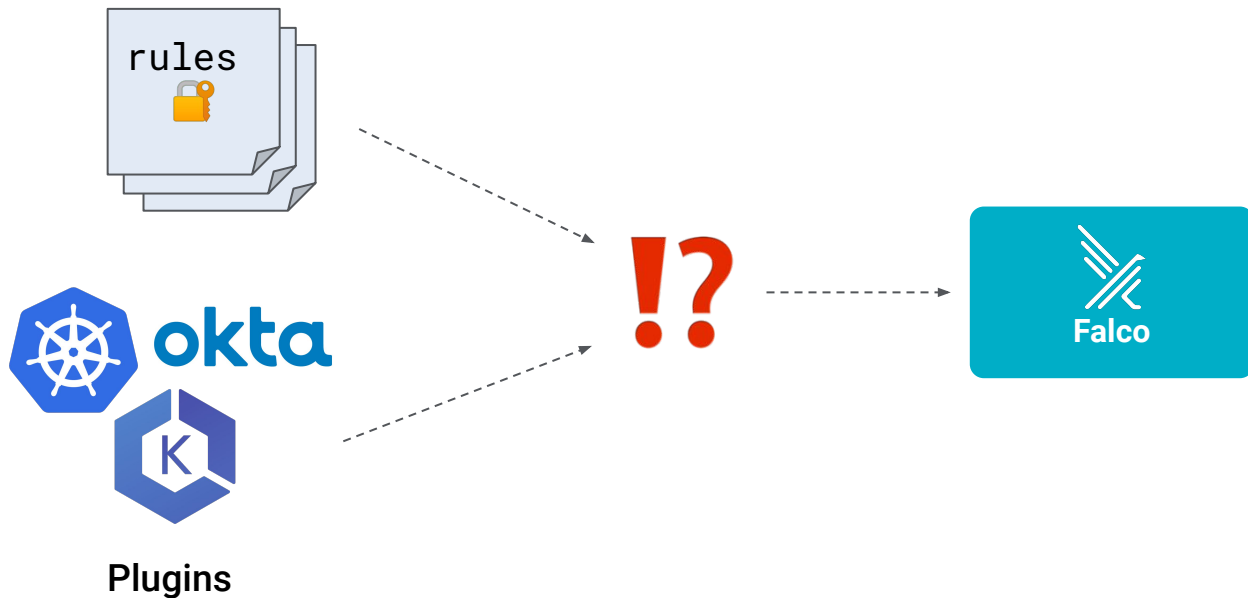


A modern probe
leveraging the most
cutting-edge eBPF features

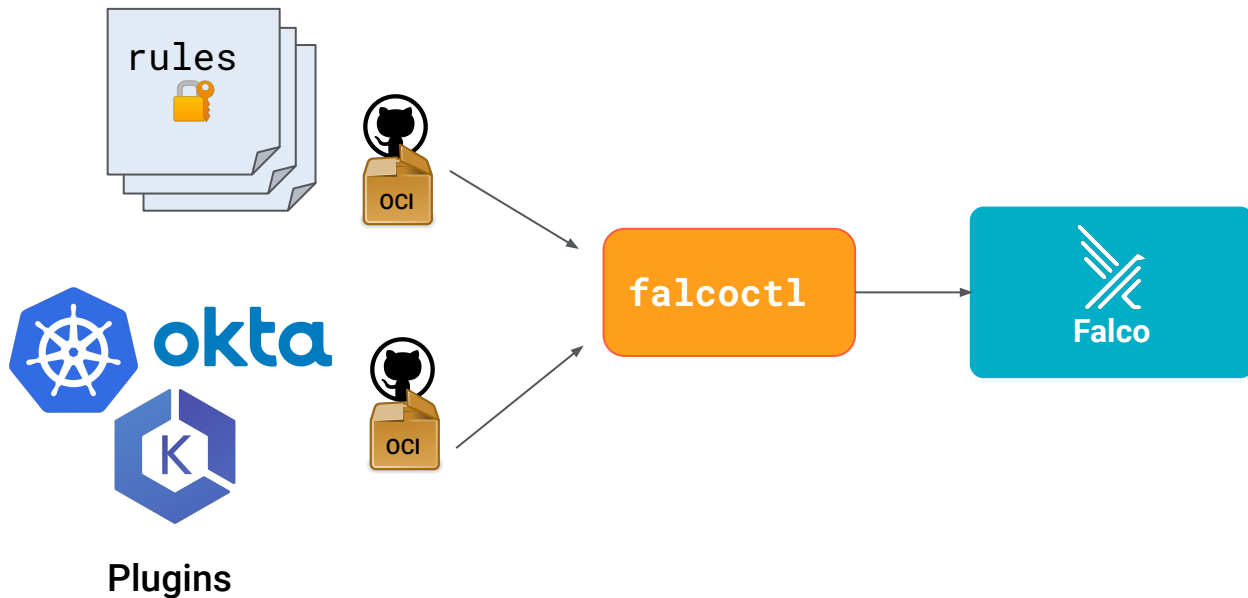
- ✓ Still under development (*soon™*)
- ✓ Already supports ~80 syscalls
- ✓ Native fine-grain unit test suite
- ✓ Safer and faster than old probe
- ✓ Easier deployment with CO-RE



Rules/Plugin management



Rules/Plugin management





Falcoctl 0.2.0 preview!

<https://github.com/falcosecurity/falcoctl>





Join the community 🤗

#falco channel on the



Kubernetes Slack 🧑💻

Falco **community call**

every Wednesday 🤝

✉ Mailing list ✉

cncf-falco-dev@lists.cncf.io

👉 github.com/falcosecurity/community 👉



Thank you!



Download the slides
and rate our talk!