



Detecting unexpected behavior and intrusions with Falco

Thomas Labarussias - Senior Developer Advocate, Sysdig
Vicente J. Jiménez Miras



Logistics

- Workshop: <https://play.instruqt.com/sysdig/invite/aivfvqywcfmr>
- Length: 90min
- QR-Code:



Agenda

- Cloud Threat Detection and Runtime Security
- Falco engine
- Falco ecosystem
- Closing remarks

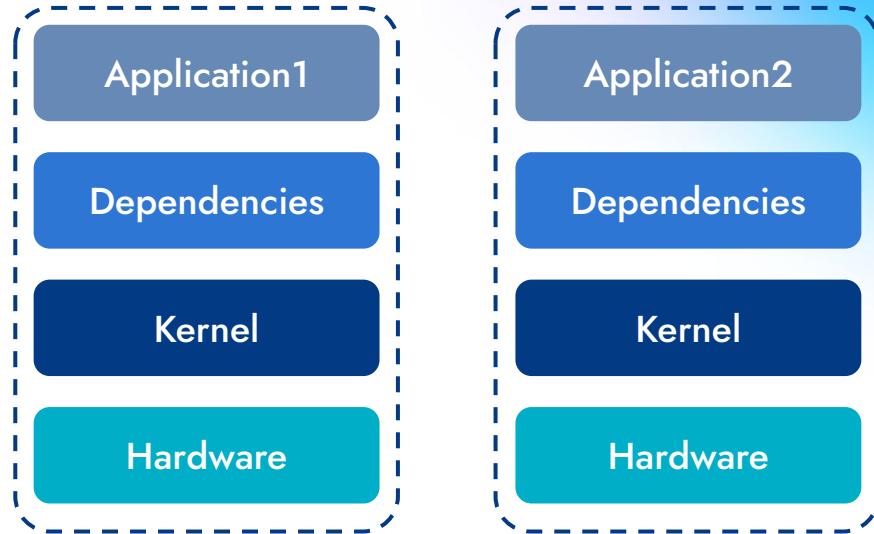
Cloud Threat Detection and Runtime Security

Microservices, Containers, and Kubernetes



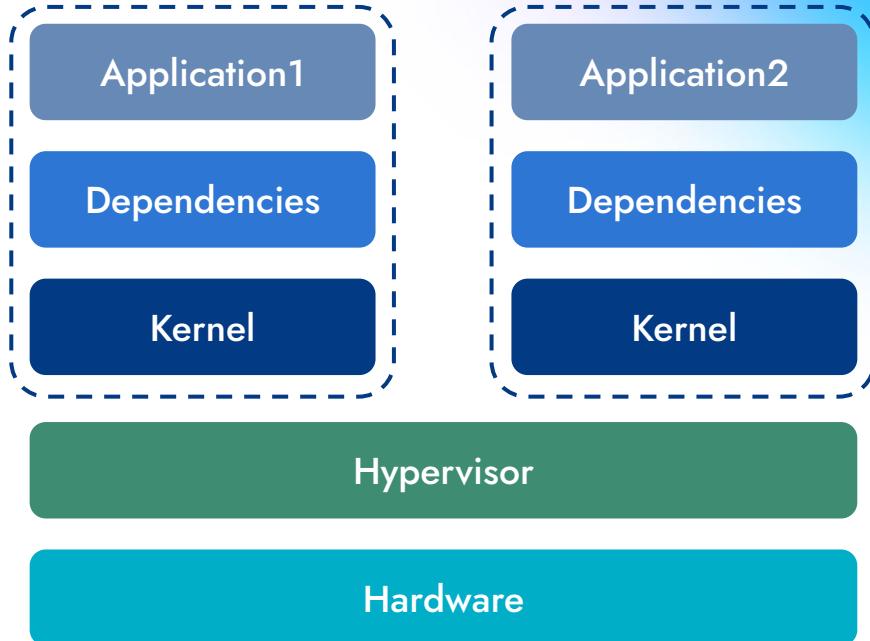
Once upon a time... dedicated servers

- Deployments took months
- Low utilization
- Not portable
- Hard to replicate



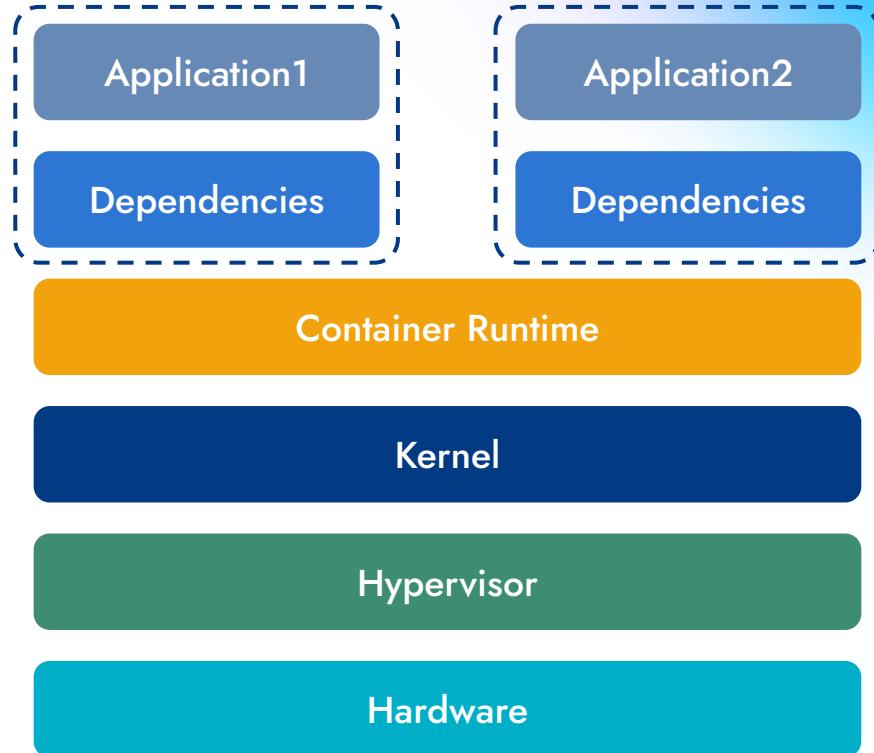
Virtualization

- Improved utilization
- Deployment took days
- Redundant kernel
- All bundled together
- Low app <-> kernel isolation



Containers

- Lightweight
- Stand-alone
- Resource efficient
- Portable execution packages
- Deploy within minutes/seconds



Rise of microservices and containers

- Need for greater flexibility, agility, scalability, and reliability
 - loosely coupled, fine-grained components.
- Microservices make it easier to:
 - build and maintain complex applications
 - scale individual services as needed, not scaling the entire system
 - adopt new technologies and tools as they become available.
 - implement changes and updates, without affecting the entire system
- Containers are a perfect fit.
- Cloud providers heavily support containers and microservices
 - easier and more cost-effective to build and scale applications.
- Containers are everywhere, but managing them at scale is challenging!

Kubernetes wins

- Kubernetes is an open-source container orchestration system
 - for automating software deployment, scaling, and management.
- Over 60% of orgs have adopted it already in 2022 (Statista research).
- Originally designed by Google,
 - the project is now maintained by the Cloud Native Computing Foundation.



CNCF - Cloud Native Computing Foundation

- Founded in 2015 to advance container technology and align the tech industry around its evolution.
- Announced alongside Kubernetes 1.0
- Part of the Linux Foundation.
- Projects have a maturity level: Sandbox, Incubated, and Graduated



What is Cloud Native?

- Cloud computing environments
- Highly scalable, flexible, and resilient applications (quick updates)
- Modern tools and techniques that support development on cloud infrastructure.
- Fast and frequent changes to applications without impacting service delivery

Cloud Threat Detection and Runtime Security

Once, there was a perimeter

You had a perimeter **guarded
by a firewall**

Detecting intrusions was your
breach indicator



Now, there is no perimeter in the cloud



Cloud providers own external connections



Cloud is exposed to the outside world



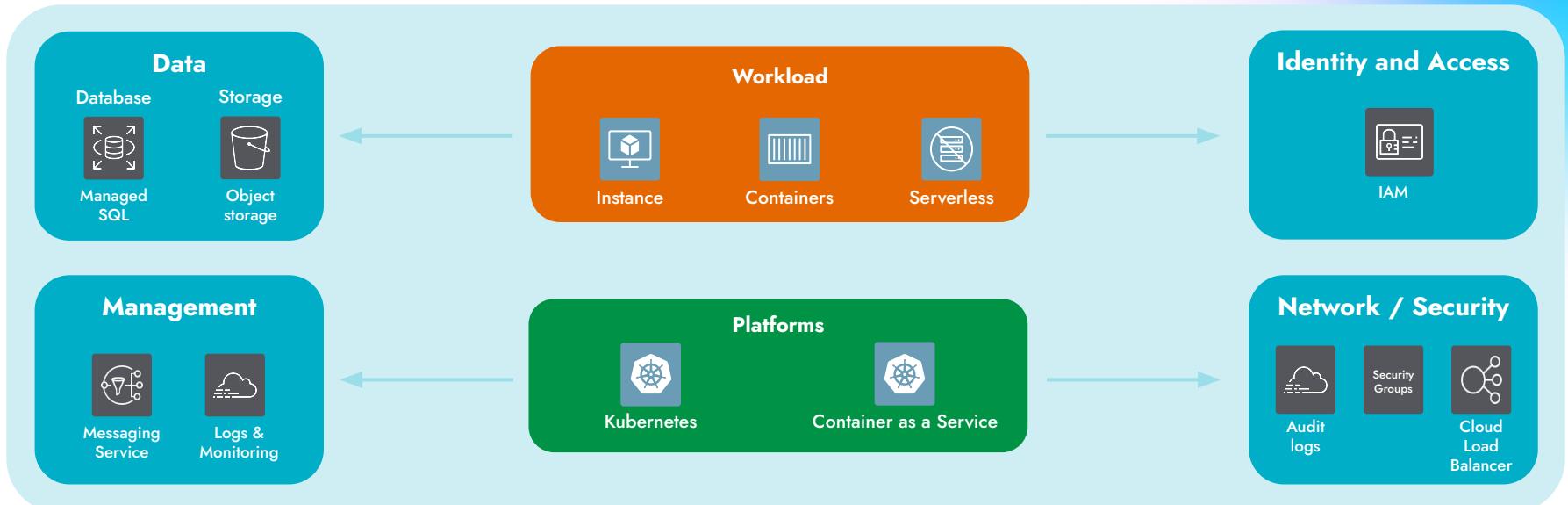
You need to control access to services your team uses



You need to detect unusual activity



Anatomy of Cloud Native Application



Cloud Infrastructure

Cloud Provider



Google Cloud

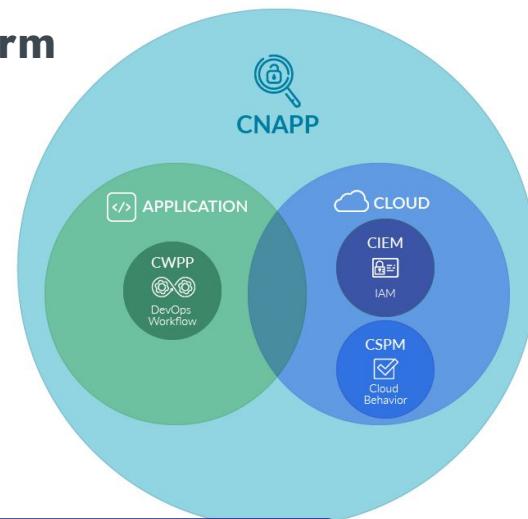


IBM Cloud

CNAPP

Cloud Native Application Protection Platform

- Vulnerability Management
- Network Security
- Posture & Compliance: CSPM, KSPM
- Entitlements Management: CIEM
- IaC Security



Then, why Runtime Security?

Why Runtime Security?

Runtime Security vs. the static approach

- Runtime behavior
 - Strict inventories
 - “Expected attacks”
 - It is not vs, but +
- Prepare for the unexpected:**
- Runtime Nature of Attacks
 - Zero-day Vulnerabilities
- (CSPM)

Example

- Log4j vulnerability was introduced in 2013.
- Reported and fixed: 2022.

Runtime Insights are a Core Capability

Protection from Source to Run

“... choose integrated CNAPP offerings that provide complete life cycle visibility across development, staging, runtime operation.”

Prioritization & Context

“...it is absolutely critical to prioritize risks identified and provide sufficient context for the developer to remediate it”

Agent & Agentless

“Favor CNAPP vendors that provide a variety of runtime visibility techniques, including traditional agents, eBPF support, snapshotting”

Without a perimeter, a security camera is more important than a good lock



Watch for changes that
create security gaps



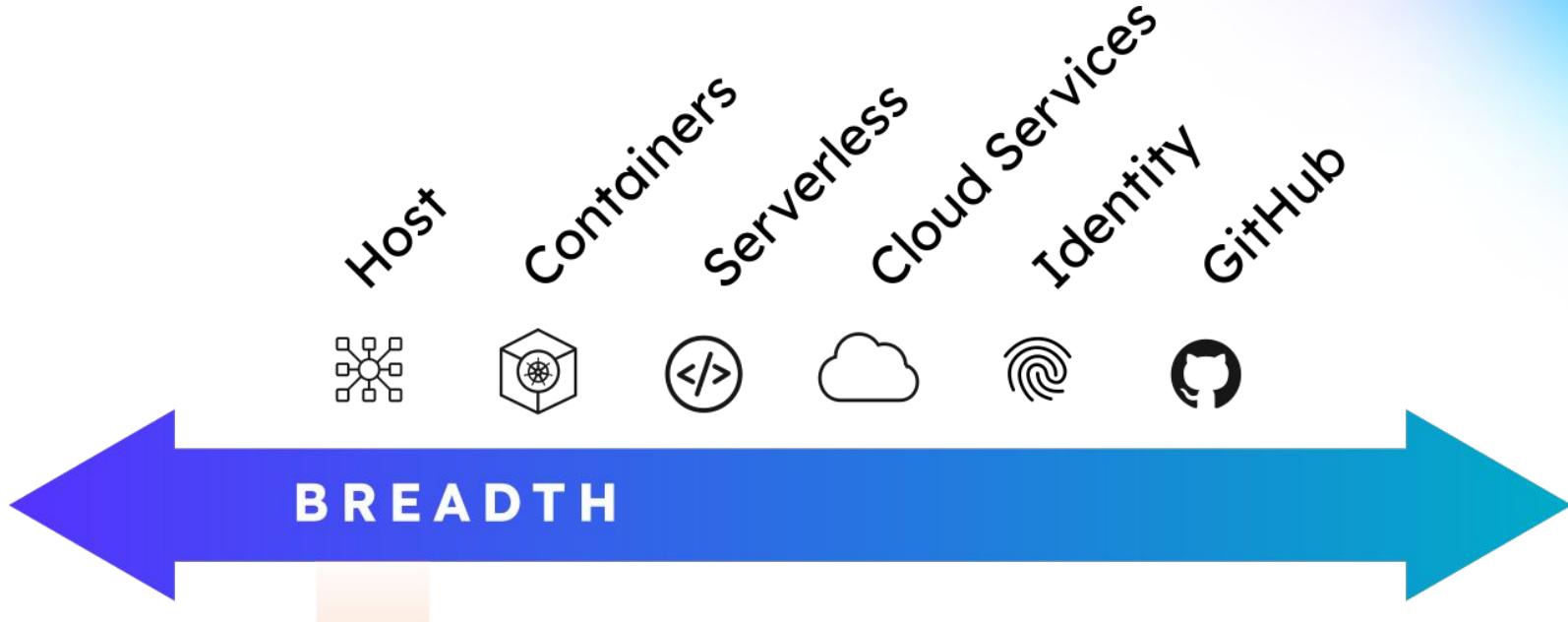
Identify intruders and
suspicious insider behavior



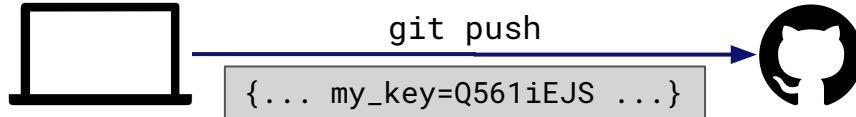
Send an alert and take
immediate action



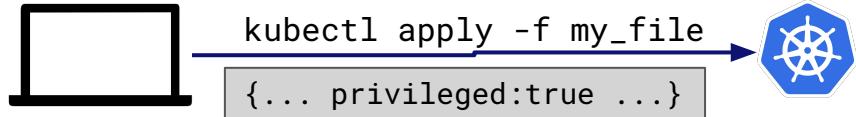
End-to-End Detection



Suspicious Activities

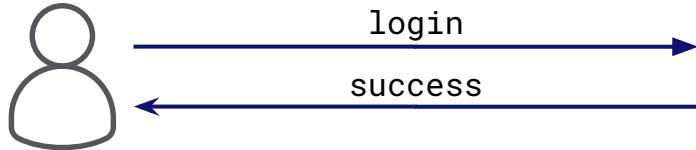


Secret pushed into a public repository.

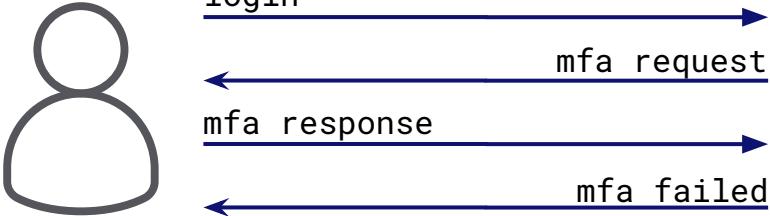


Create privileged pod.

Suspicious Activities

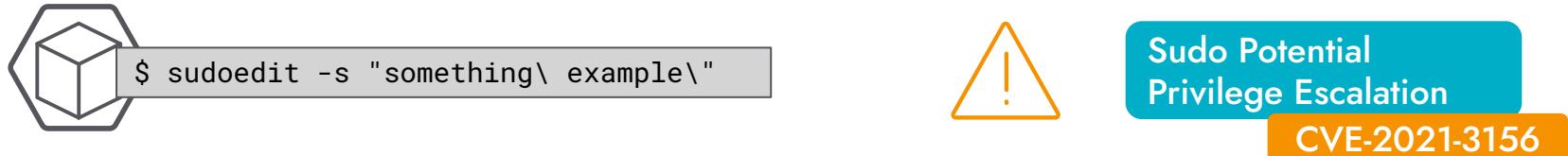


Console login without MFA



Too many failed MFA in the last 5m

Suspicious Activities



Falco

Falco

Falco is an **open source** runtime security solution for **threat detection** across **Kubernetes**, containers, hosts and **the cloud**.

CNCF Incubation-Level Project

(the graduation will be official in December 2023)

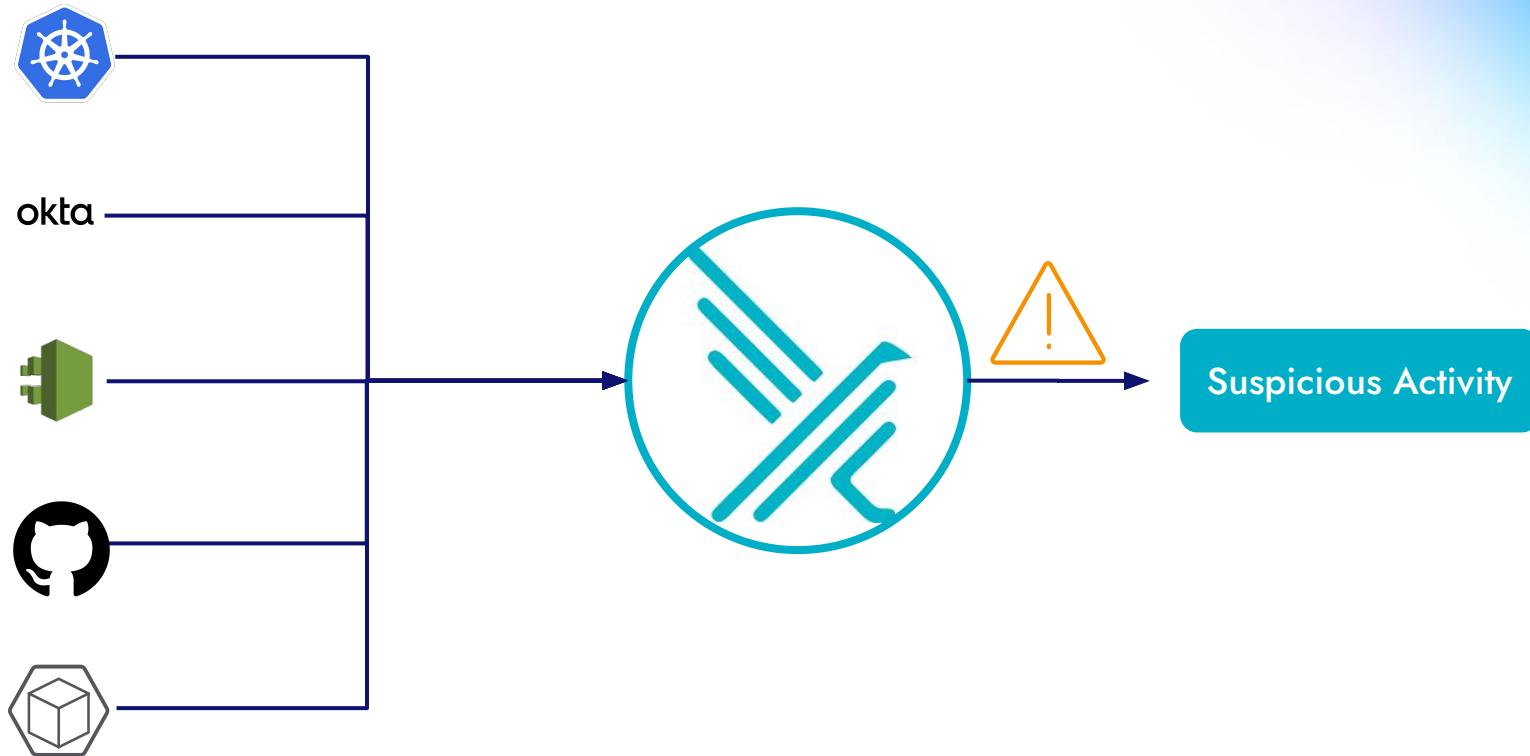
★ 6.7k

 60M+ pulls



**CLOUD NATIVE
COMPUTING FOUNDATION**

Falco overview

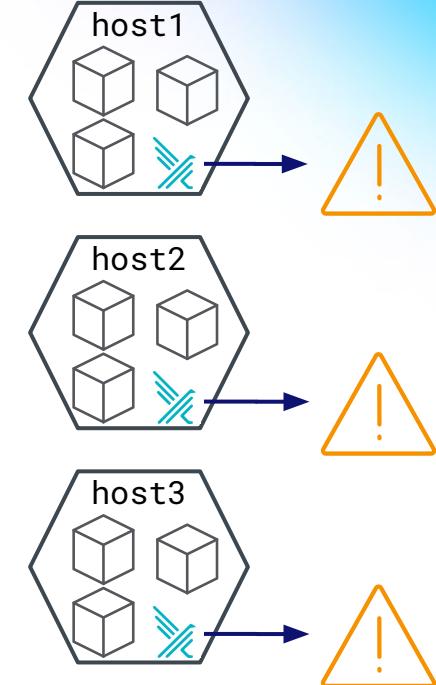
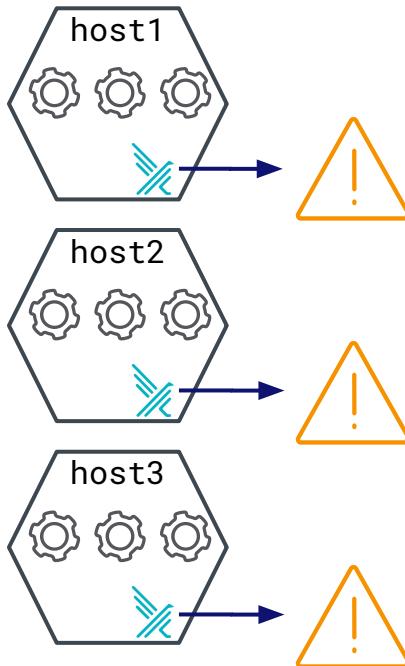
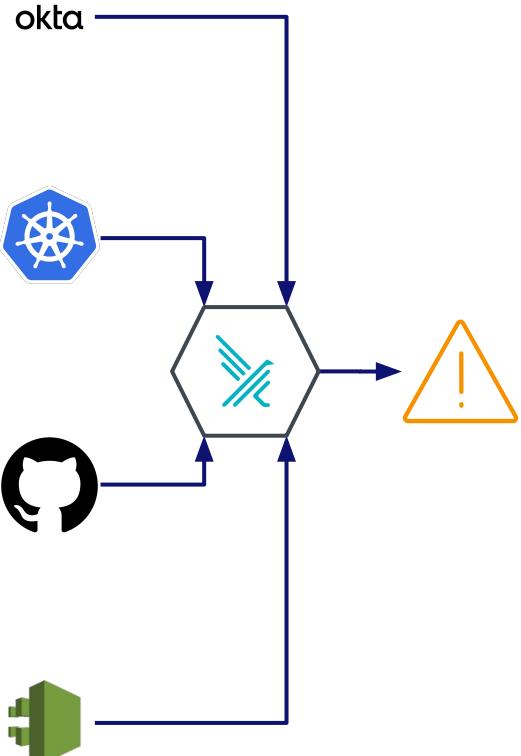


Falco



```
2022-04-07T12:51:08: Notice A shell was spawned in a container with an attached terminal (user=root user_loginuid=-1 elastic_borg (id=a10bd3b1b2a8) shell=bash parent=<NA> cmdline=bash terminal=34816 container_id=a10bd3b1b2a8 image=ubuntu)
2022-04-07T12:51:41: Warning Netcat runs inside container that allows remote code execution
(user=root user_loginuid=-1 command=nc -e container_id=a10bd3b1b2a8 container_name=elastic_borg
image=ubuntu:latest)
```

Falco deployment examples



Set up Falco

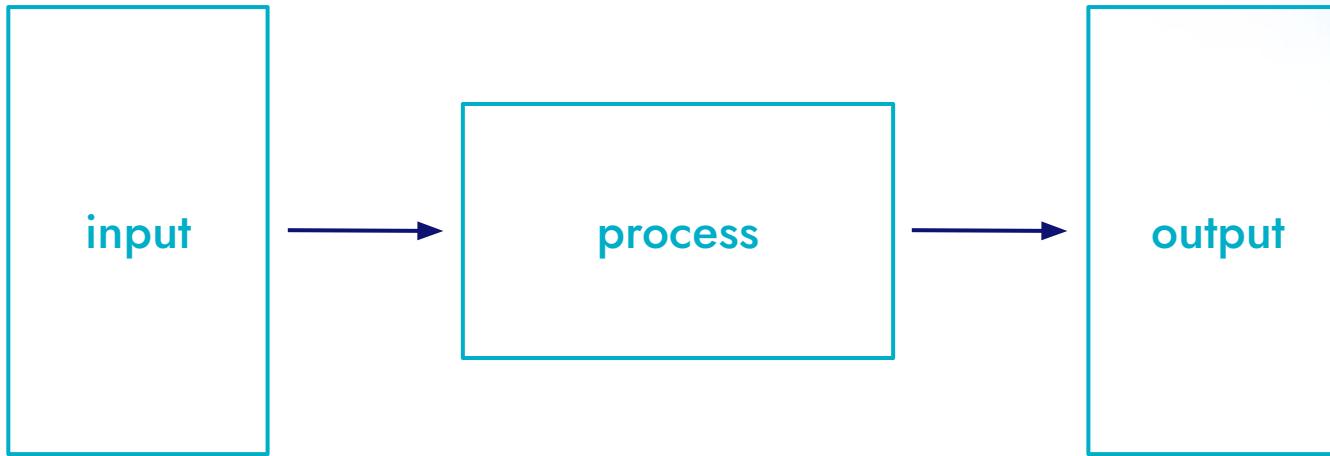


Lab time!

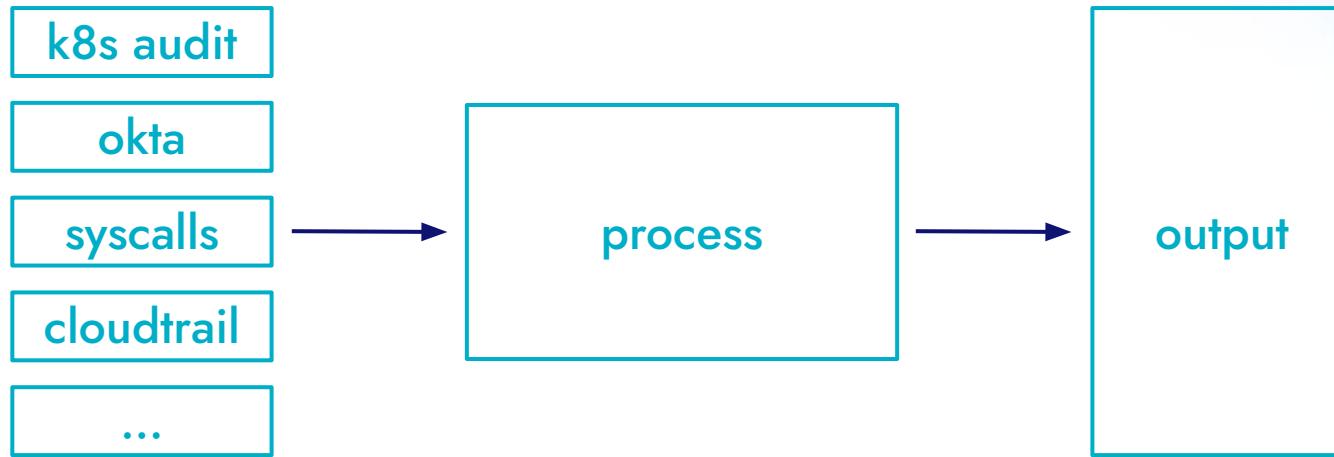


Falco engine

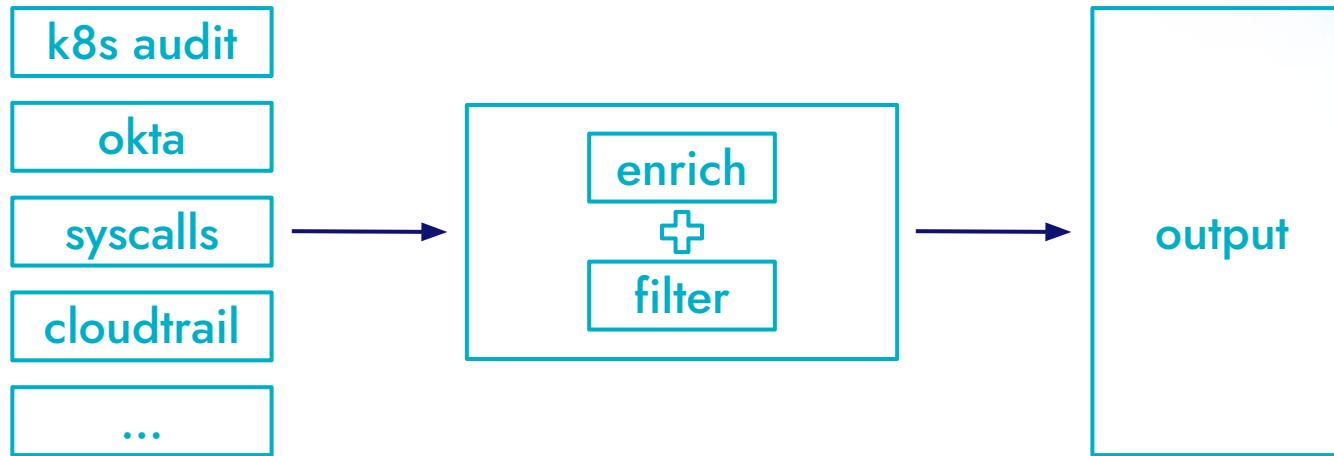
Falco architecture



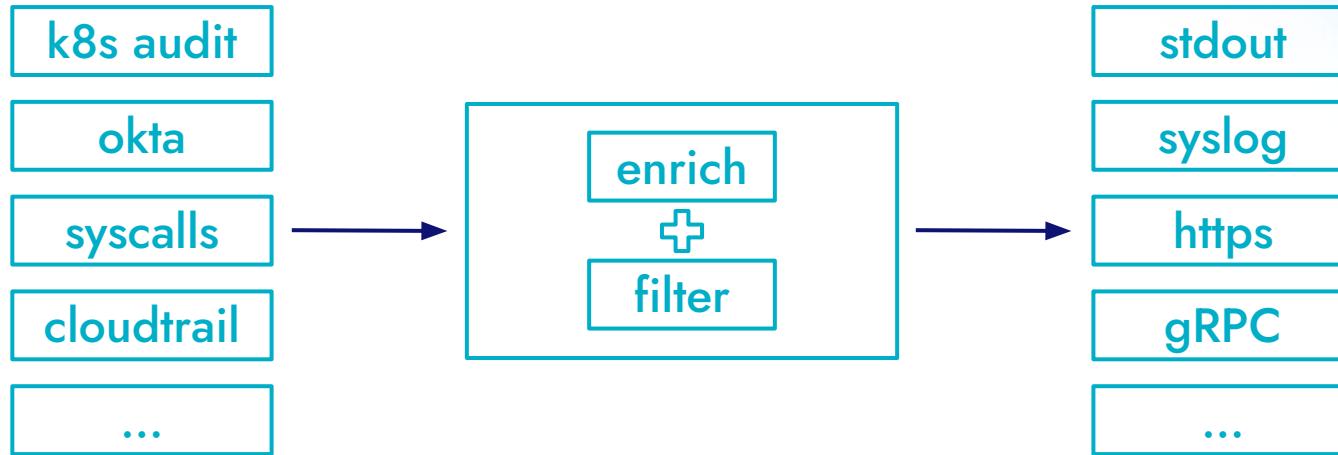
Falco architecture



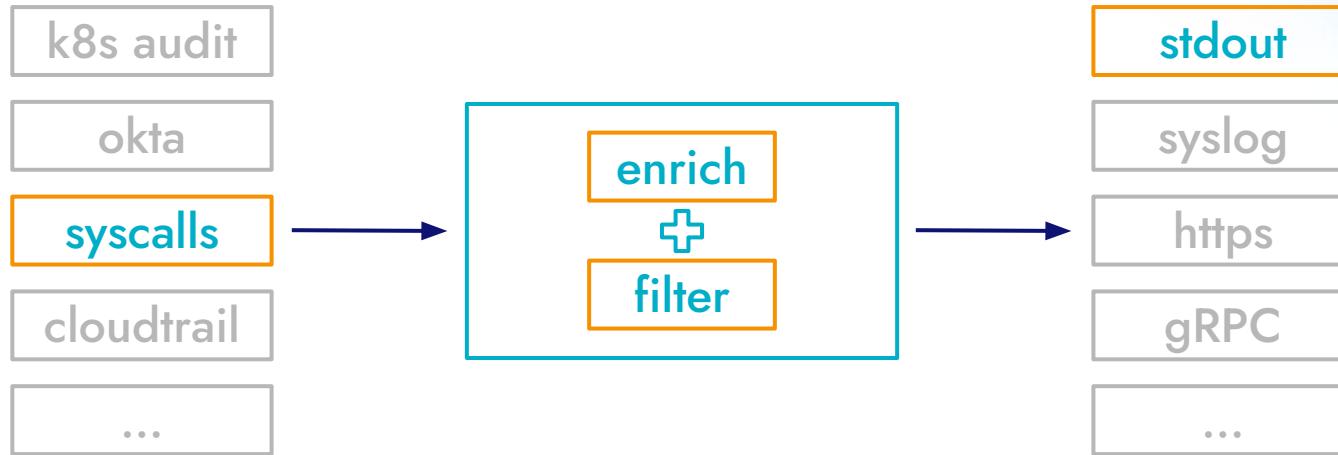
Falco architecture



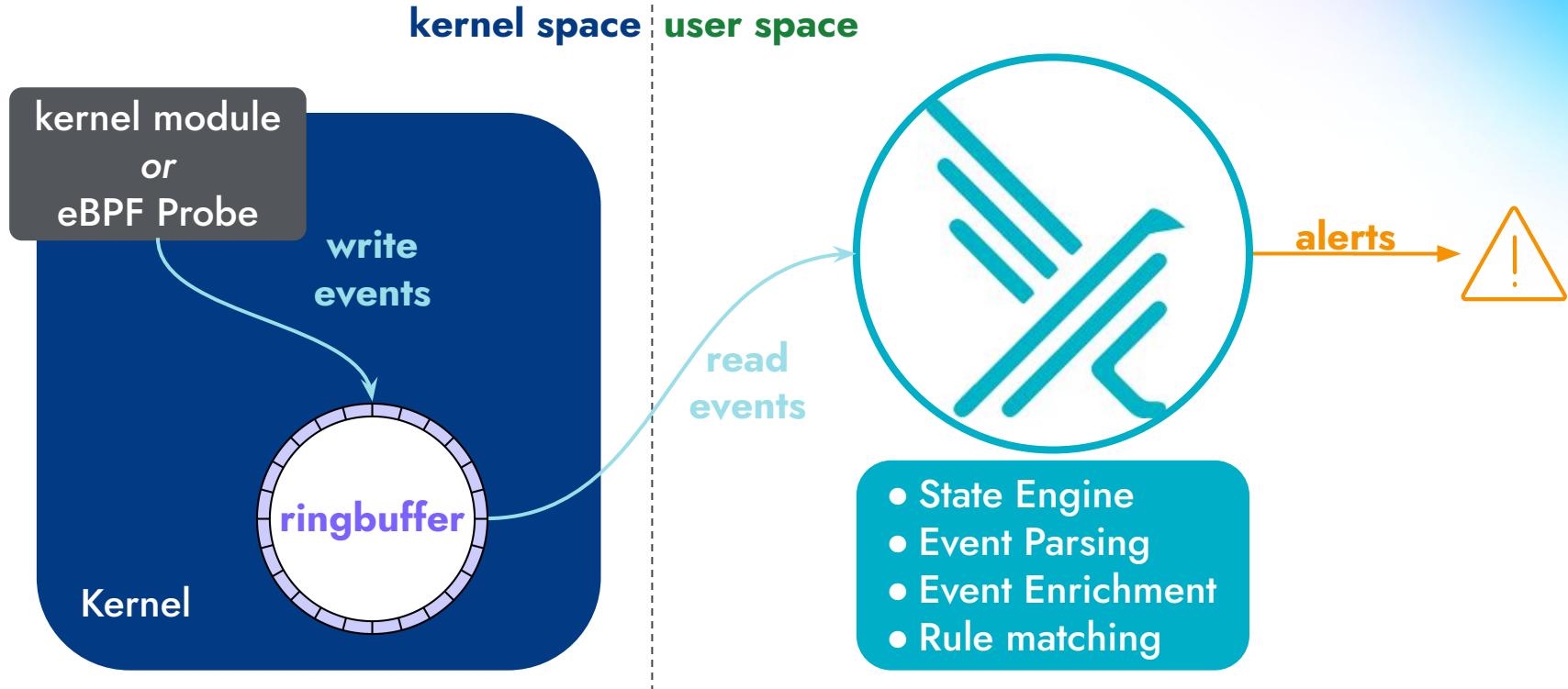
Falco architecture



Falco architecture



Falco Syscall Architecture Overview



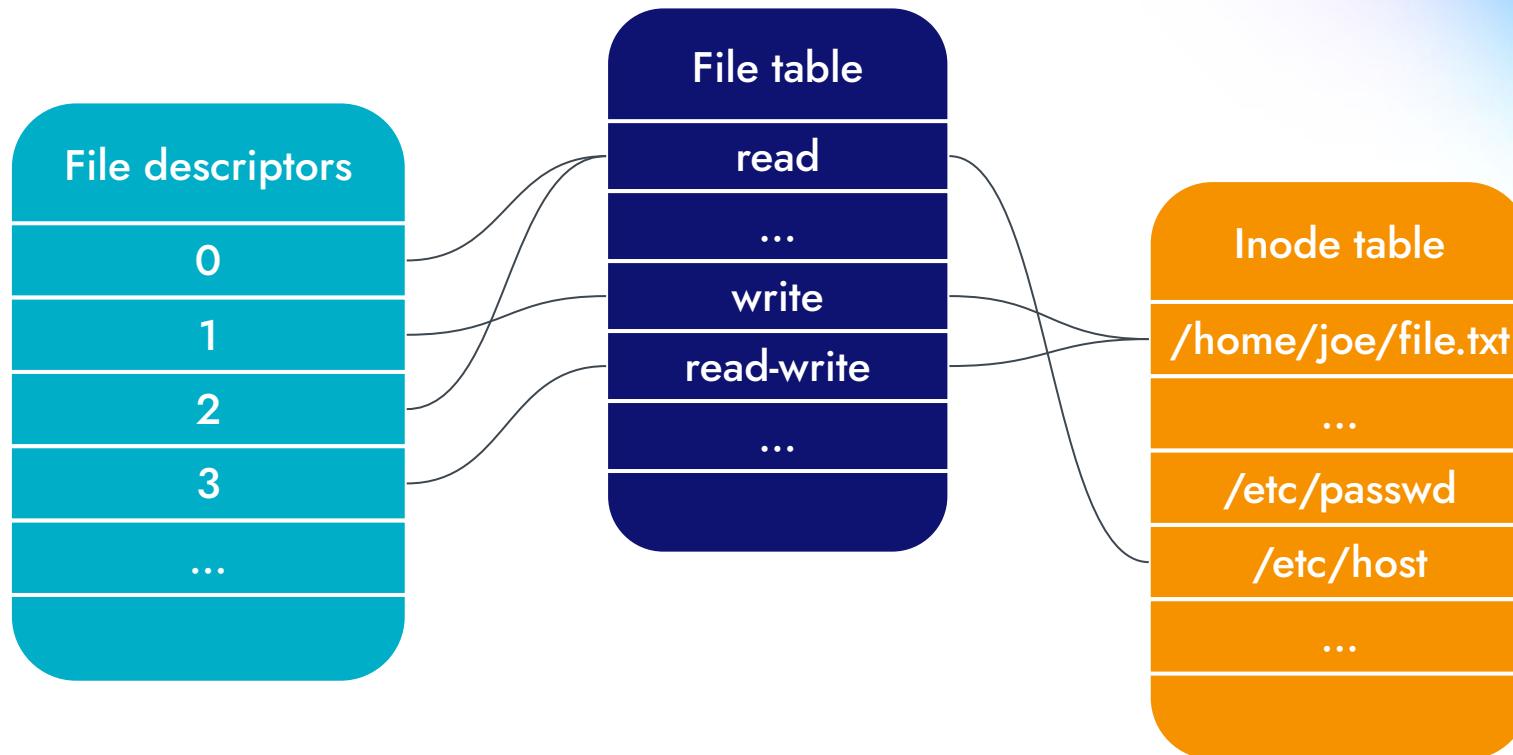


- Extended Berkeley Packet Filter.
- Extend the kernel capabilities safely
 - without changing kernel source code
 - without loading kernel modules.

**Kernel instrumentation
made simple!**

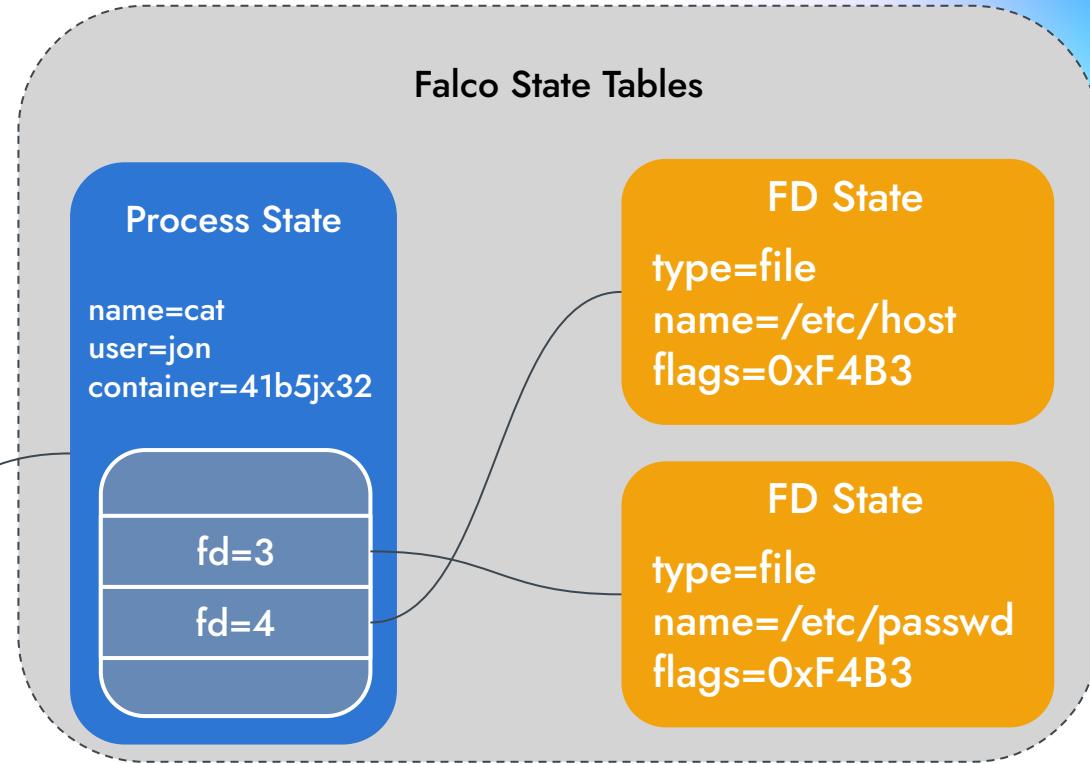
**Modern, low-overhead, production-ready
observability for monitoring and security
in containers and Linux systems.**

Navigating the Linux File System



Falco State

Linux Process Table
pid=472
pid=473
pid=474
pid=475



Falco default rules

- Falco ships with more than 80 default rules:
 - Privilege escalation
 - R/W to sensitive directories
 - Executing shell
 - Execute SSH binaries
 - Mutating binaries
 - Creating symlinks
 - ...

Falco syntax

- **rule**: Terminal shell in container
desc: A shell has been spawned in a container.
condition: >
 spawned_process and container and shell_procs
output: >
 A shell was spawned in a container (user=%user.name
 user_loginuid=%user.loginuid %container.info shell=%proc.name
 parent=%proc.pname cmdline=%proc.cmdline container_id=%container.id)

Falco syntax

- **rule**: Terminal shell in container
desc: A shell has been spawned in
condition: >
 spawned_process and container are
output: >
 A shell was spawned in a container
 user_loginuid=%user.loginuid %container.id
 parent=%proc.pname cmdline=%proc.cmdline

- **list**: shell_binaries
 - items**: [ash, bash, csh, ksh, sh, tcsh, zsh, dash]
- **macro**: shell_procs
 - condition**: proc.name in (shell_binaries)
- **macro**: container
 - condition**: (container.id != host)
- **macro**: spawned_process
 - condition**: >
 evt.type in (execve, execveat)
 and evt.dir==

Macros and Lists

- **Macros** allow you to define conditions and reuse them wherever you want.
- **Lists** help you organize your rules files with naming and segmentation.
- They have four main benefits:
 - code reuse
 - avoid long strings of conditions
 - rules are easier to understand
 - easier to extend

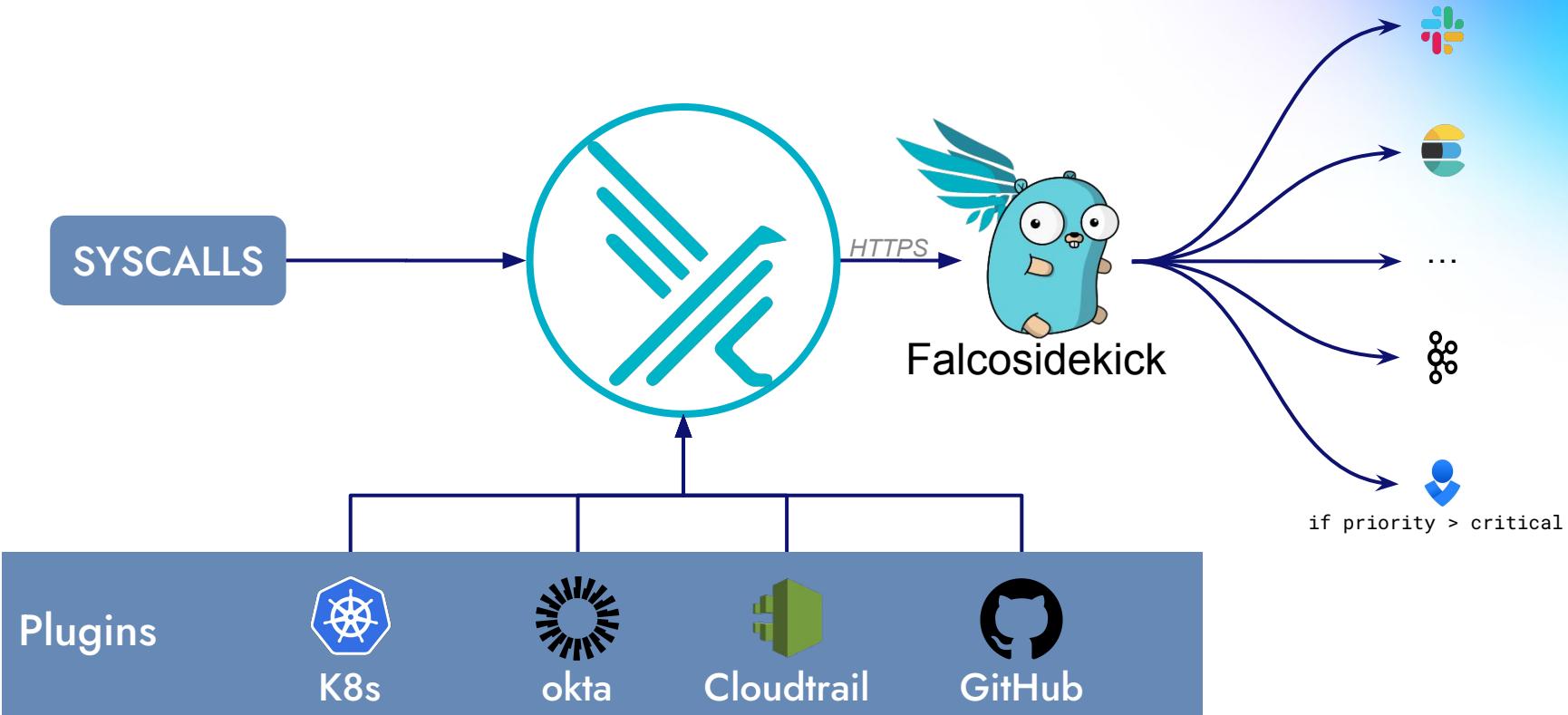
Falco default rules



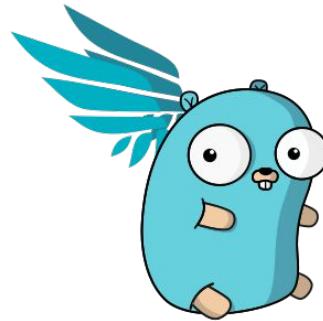
Lab time!

Falco ecosystem

Falco ecosystem



Falcosidekick



chat



logs



queue/streaming



faas



metrics



alerting

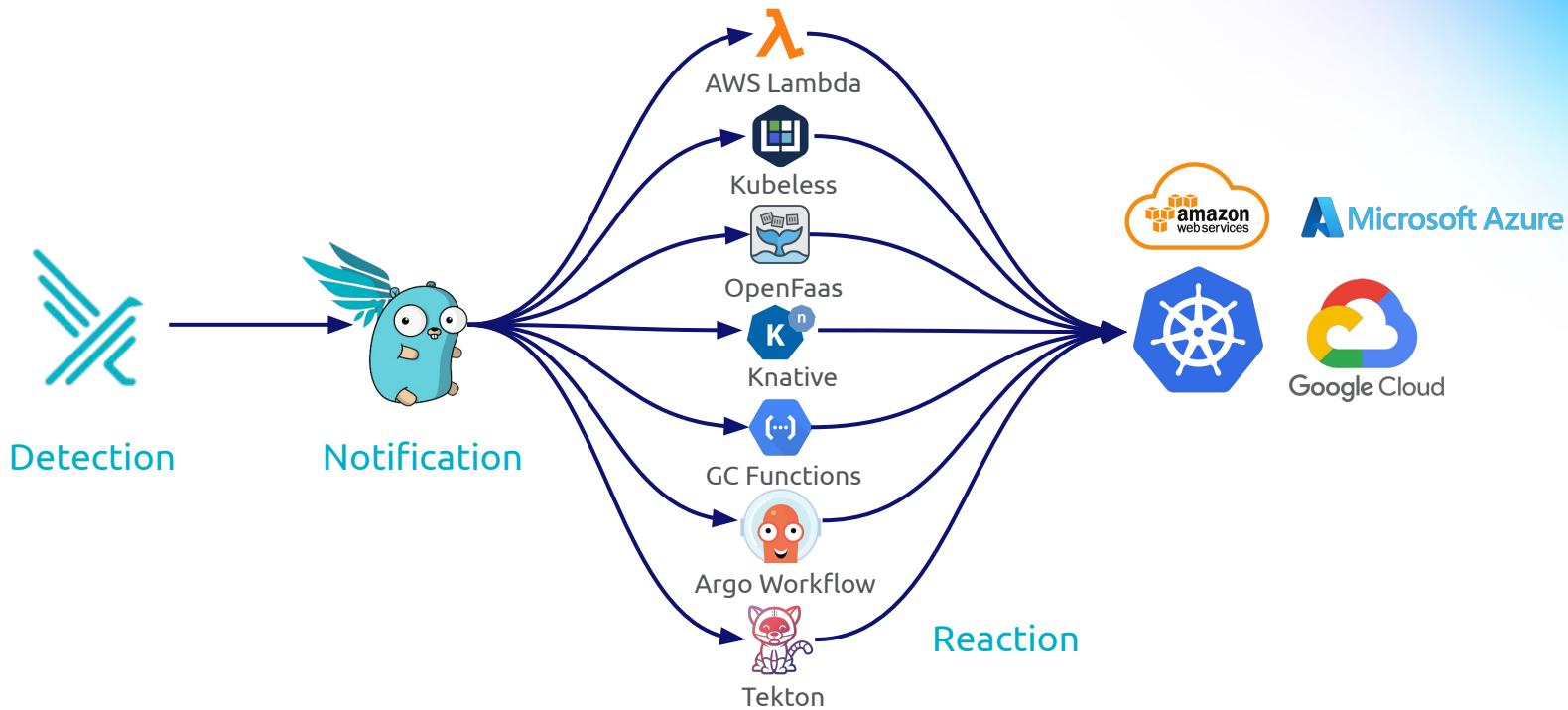


storage



and more ...

React to events



Falcosidekick install

Standalone:

```
helm repo add falcosecurity https://falcosecurity.github.io/charts  
helm repo update  
  
helm install falcosidekick -n falco --set config.debug=true falcosecurity/falcosidekick
```

With Falco:

```
helm install falco -n falco falcosecurity/falco \  
  --set falcosidekick.enabled=true \  
  --set falcosidekick.webui.enabled=true
```

Event generator

- Generates a variety of suspect actions that are detected by Falco rulesets.
- Good to test Falco rulesets:
 - syscalls
 - kubernetes audit
- Run it within Docker or Kubernetes,
 - as some commands might alter your system.

```
docker run -it --rm falcosecurity/event-generator run
```

```
helm install event-generator falcosecurity/event-generator \
--namespace event-generator \
--create-namespace \
--set config.actions=""
```

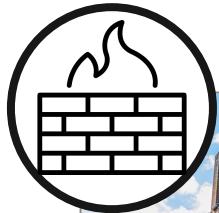
Falco ecosystem



Lab time!

Closing remarks

Runtime security

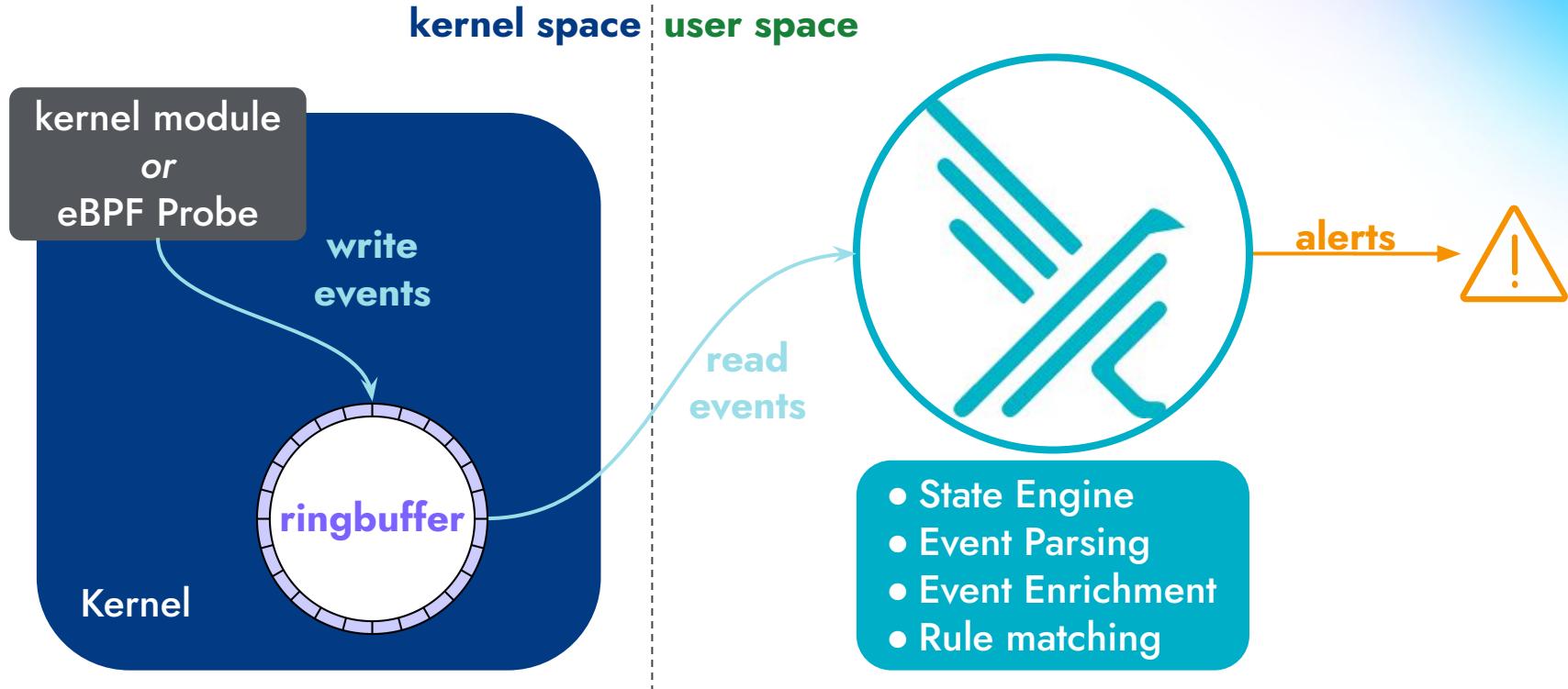


Guard perimeter



Detect unusual activities

Falco Syscall Architecture Overview



Falco rules

- **rule**: Terminal shell in container

desc: A shell has been spawned in a container.

condition: >

spawned_process and container and shell_procs

output: >

A shell was spawned in a container (user=%user.name

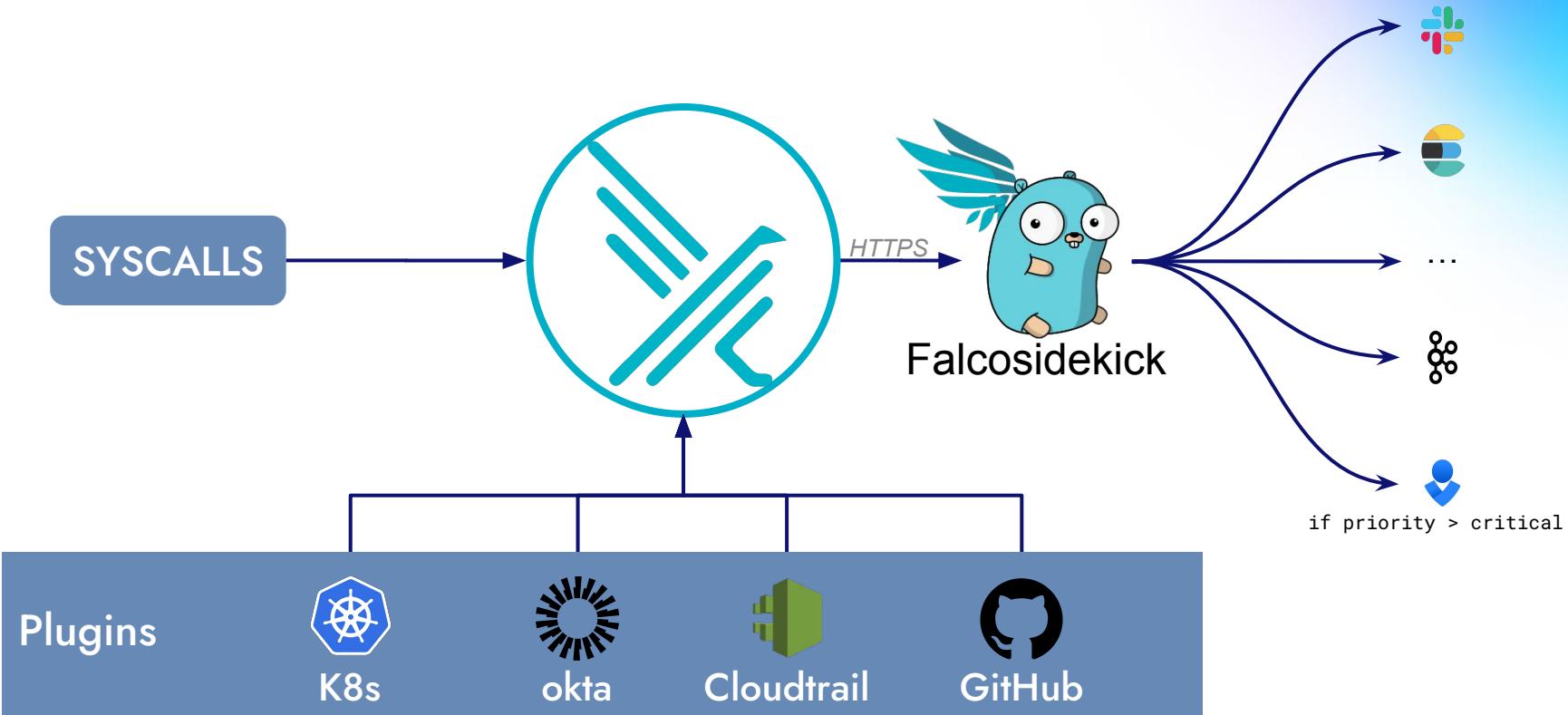
user_loginuid=%user.loginuid %container.info shell=%proc.name

parent=%proc.pname cmdline=%proc.cmdline container_id=%container.id)

priority: WARNING

tags: [container, shell, mitre_execution]

Falco ecosystem



Reference

"Practical Cloud Native Security with Falco", O'Reilly book

<https://falco.org/docs>

<https://falco.org/training>

<https://falco.org/blog/extend-falco-outputs-with-falcosidekick/>

Survey

<https://bit.ly/falcosurveypdx>



sysdig

Seeing is Securing

Color Usage



Color Use Percentage

This graph shows the balance of color usage that should be considered throughout when creating slide decks. Sysdig blues should always be most prevalent, using purples as compliment colors for gradients, then mixes of greens for gradients or shape compositions, and finally oranges and yellows as accent colors, only used sparingly to add brightness and energy.



Red

Severity Colors

Colors are frequently used to indicate the severity of a vulnerability or other security issue. Use these colors to reflect severity in your presentations.



This red is not a part of the Sysdig color palette, and should only be used for specific cases like showing error states.