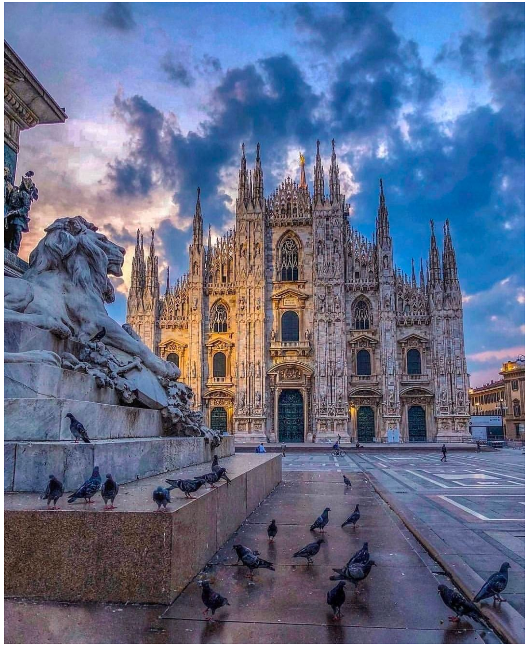
Falco + Falcosidekick = Create your own Kubernetes Response Engine

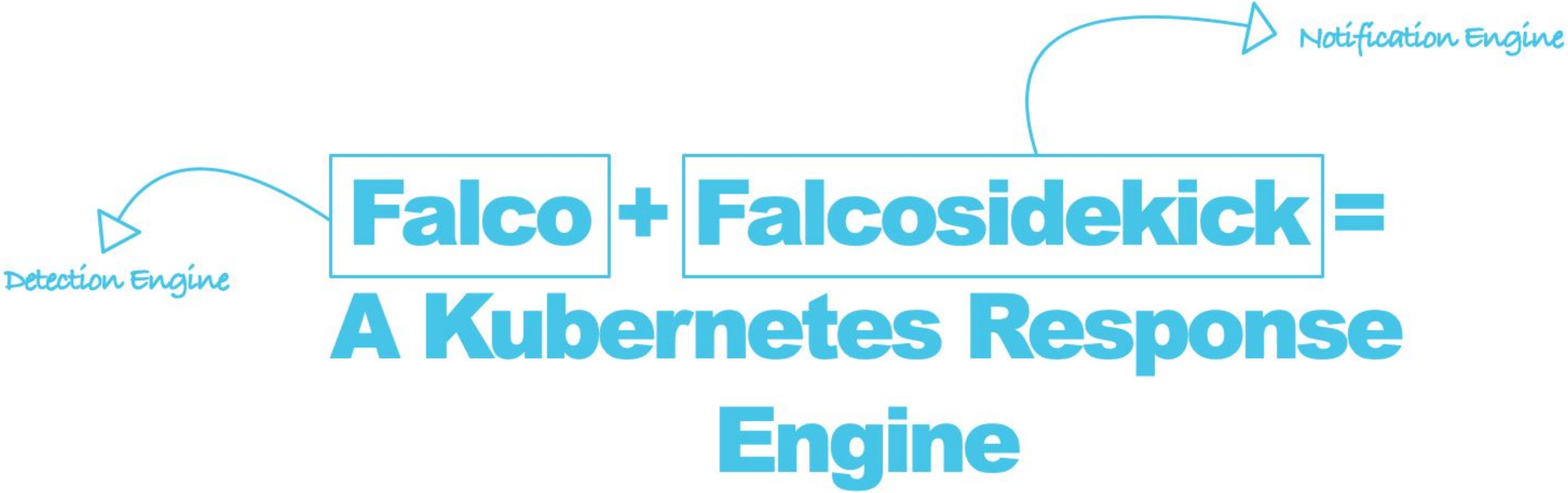
HackInBo®
Winter 2021 Edition
17ª EDIZIONE

#Whoami

- Chierici Stefano
- Security Researcher @ Sysdig
- @Darryk10
- https://github.com/darryk10
- Falco Contributor



HACK IN BO®
Winter 2021 Edition
17° EDIZIONE

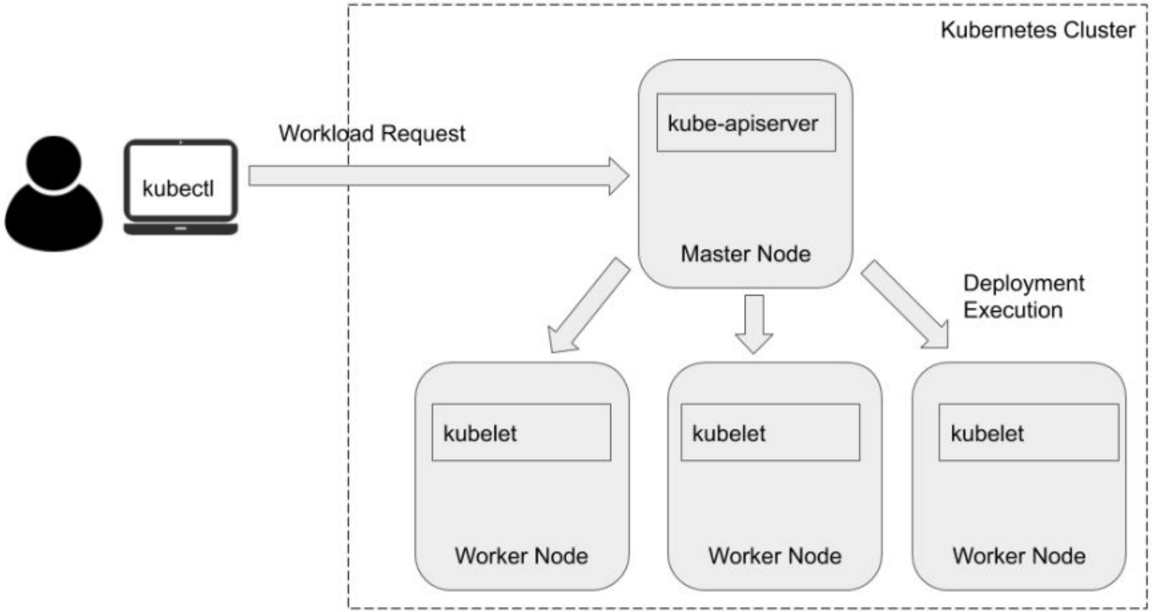


Falco + Falcosidekick = A Kubernetes Response Engine

Detection Engine

Notification Engine

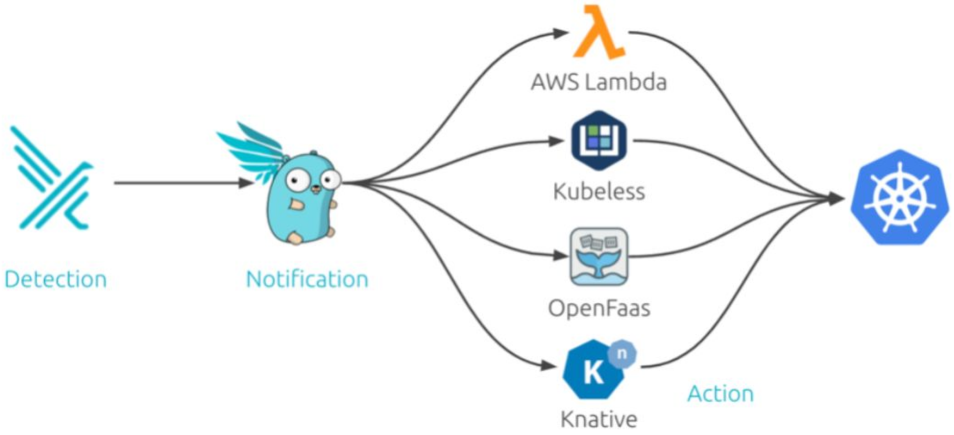
Kubernetes Infrastructure



https://github.com/PacktPublishing/Learn-Kubernetes-Security

Why we need a K8s Response Engine?

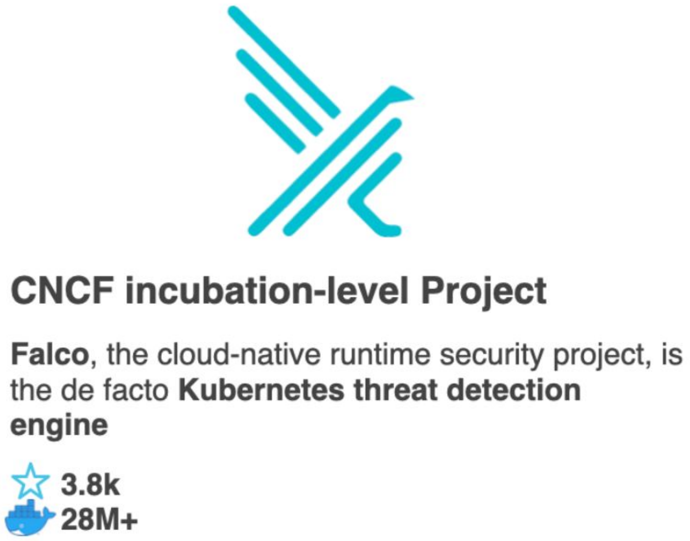
- **Automate Response**
- **Faster incident detection and reaction times**
- **Scalability**
- **Simplified management**



#Falco

Falco, a CNCF Project

- Created Originally by Sysdig
- Donated to CNCF in 2018
- Currently run independently by the Falco community
- Incubation level Project



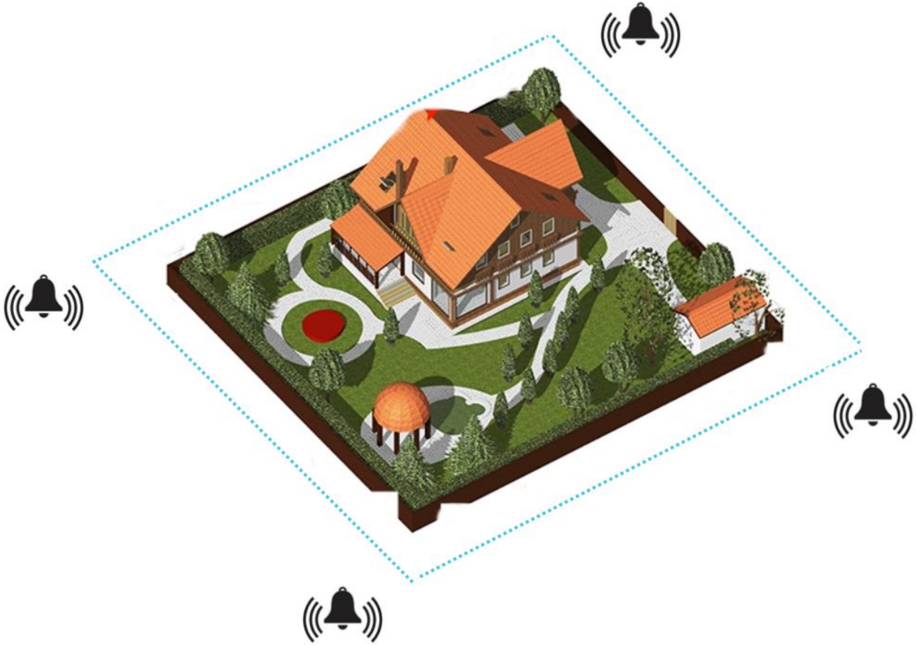
CNCF incubation-level Project

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

☆ **3.8k**

28M+

Why runtime security?



Prevention Intrusion

- Fences
- Door locks
- Perimeter sensors
- Windows and doors sensors
- External Camera

↓

- Passwords
- MFA
- Container Image Scanning
- Fixing Software Vulnerabilities
- Firewalls

Why runtime security?

Why runtime security?

Detection Intrusion

- Motion Sensors
- Interior Cameras
- Volumetric Sensors

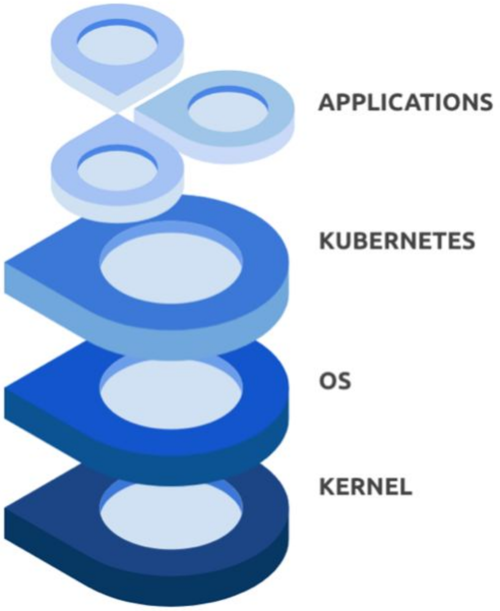
Why runtime security?

Why Syscall

When you run a program you are generating system call.

System calls are how a program enters the kernel to perform some task.

- processes
- network
- file IO
- much more...



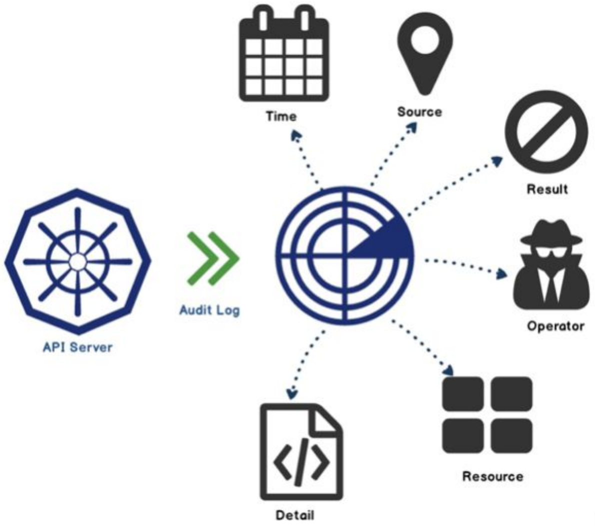
Not Just Syscall

What if the program is launched in a k8s container?

System calls are as important as k8s audit

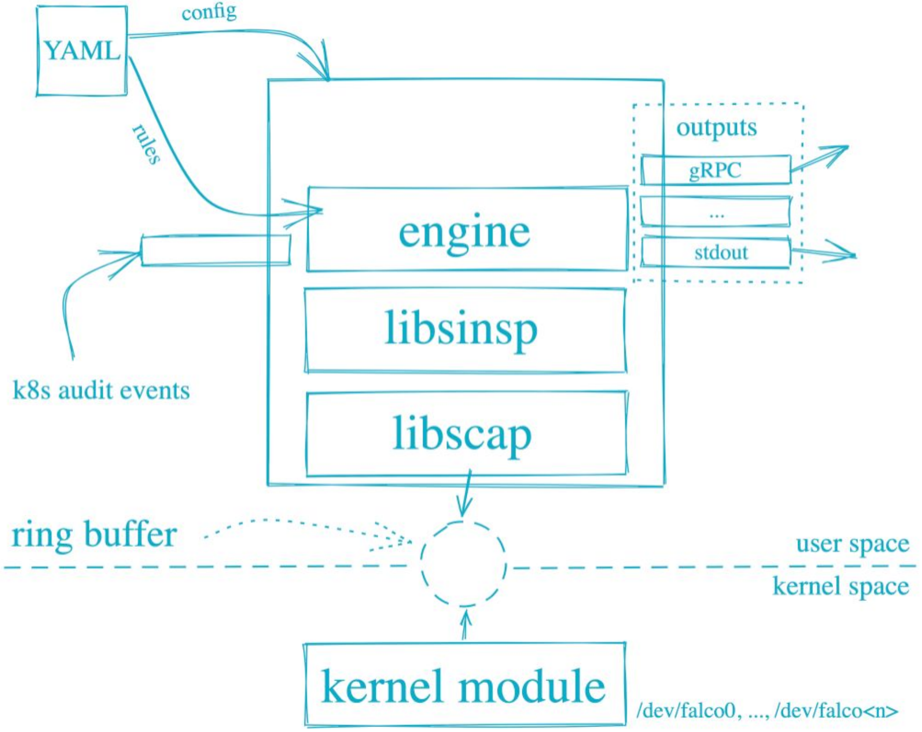
- what happened?
- when did it happen?
- who initiated it?
- on what did it happen?
- where was it observed?
- from where was it initiated?
- to where was it going?

K8s Audit

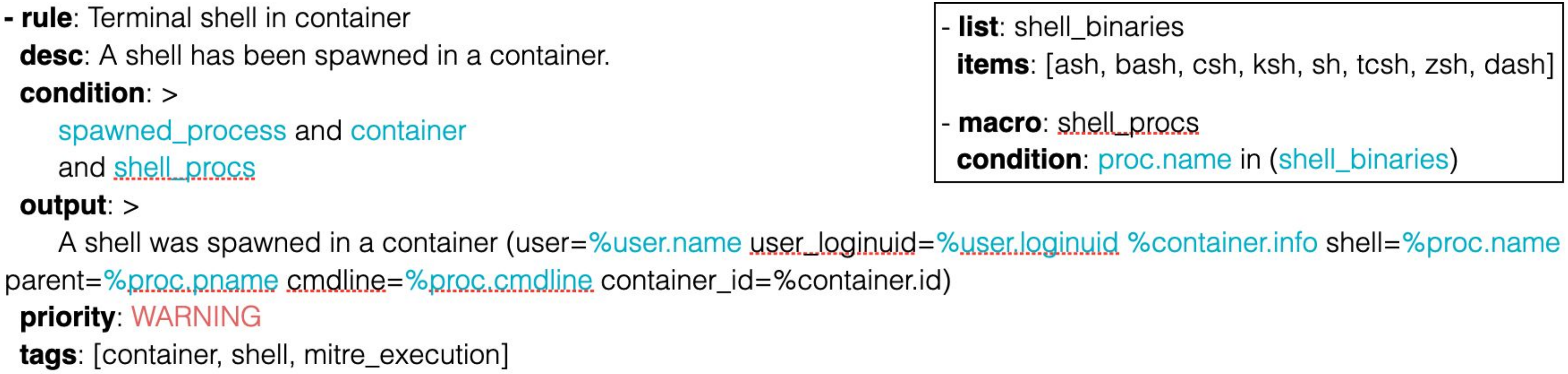


HackInBo® Winter 2021 Edition
17° EDIZIONE

#Falco


YAML
config
rules
outputs
gRPC
...
stdout
engine
libsinsp
libscap
k8s audit events
ring buffer
user space
kernel space
kernel module
/dev/falco0, ..., /dev/falco<n>

Falco Rules

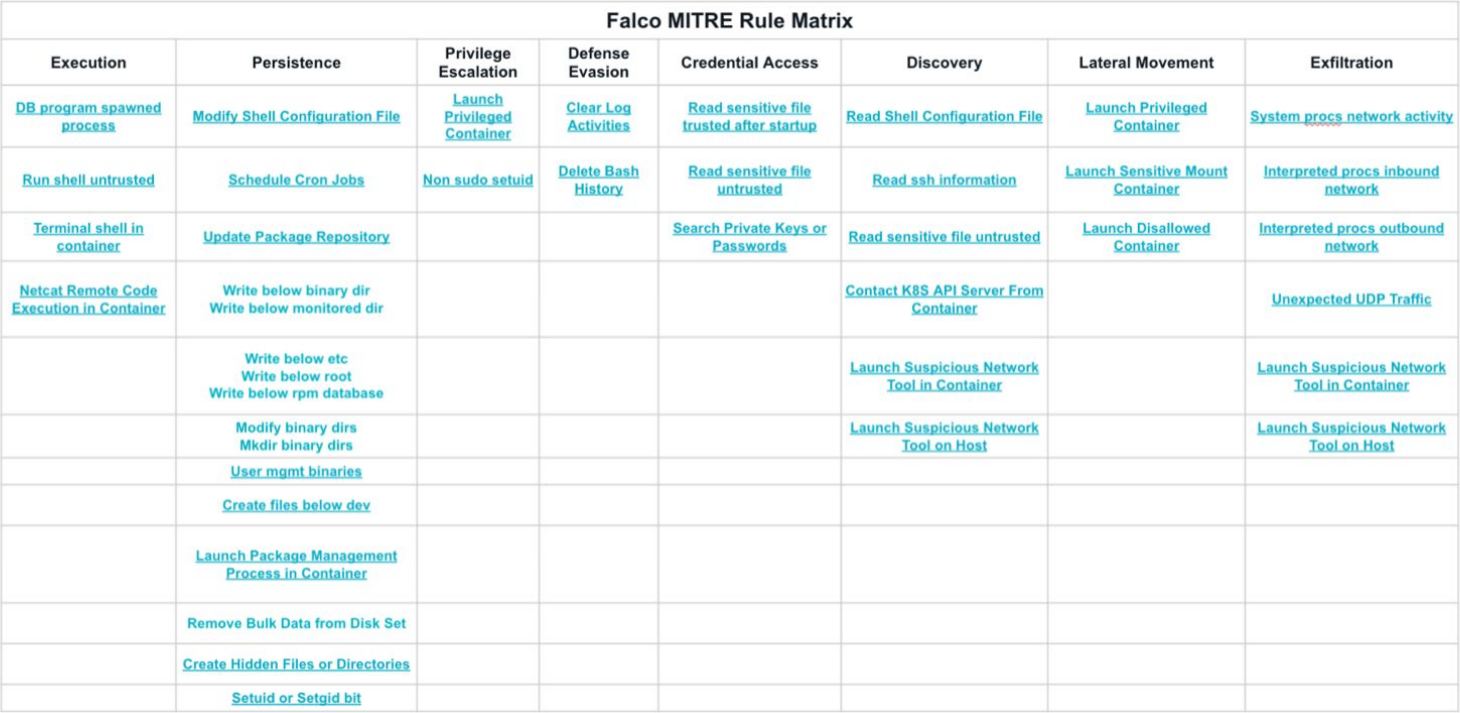


```
- rule: Terminal shell in container
  desc: A shell has been spawned in a container.
  condition: >
      spawned_process and container
      and shell_procs
  output: >
      A shell was spawned in a container (user=%user.name user_loginuid=%user.loginuid %container.info shell=%proc.name
parent=%proc.pname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

```
- list: shell_binaries
  items: [ash, bash, csh, ksh, sh, tcsh, zsh, dash]

- macro: shell_procs
  condition: proc.name in (shell_binaries)
```

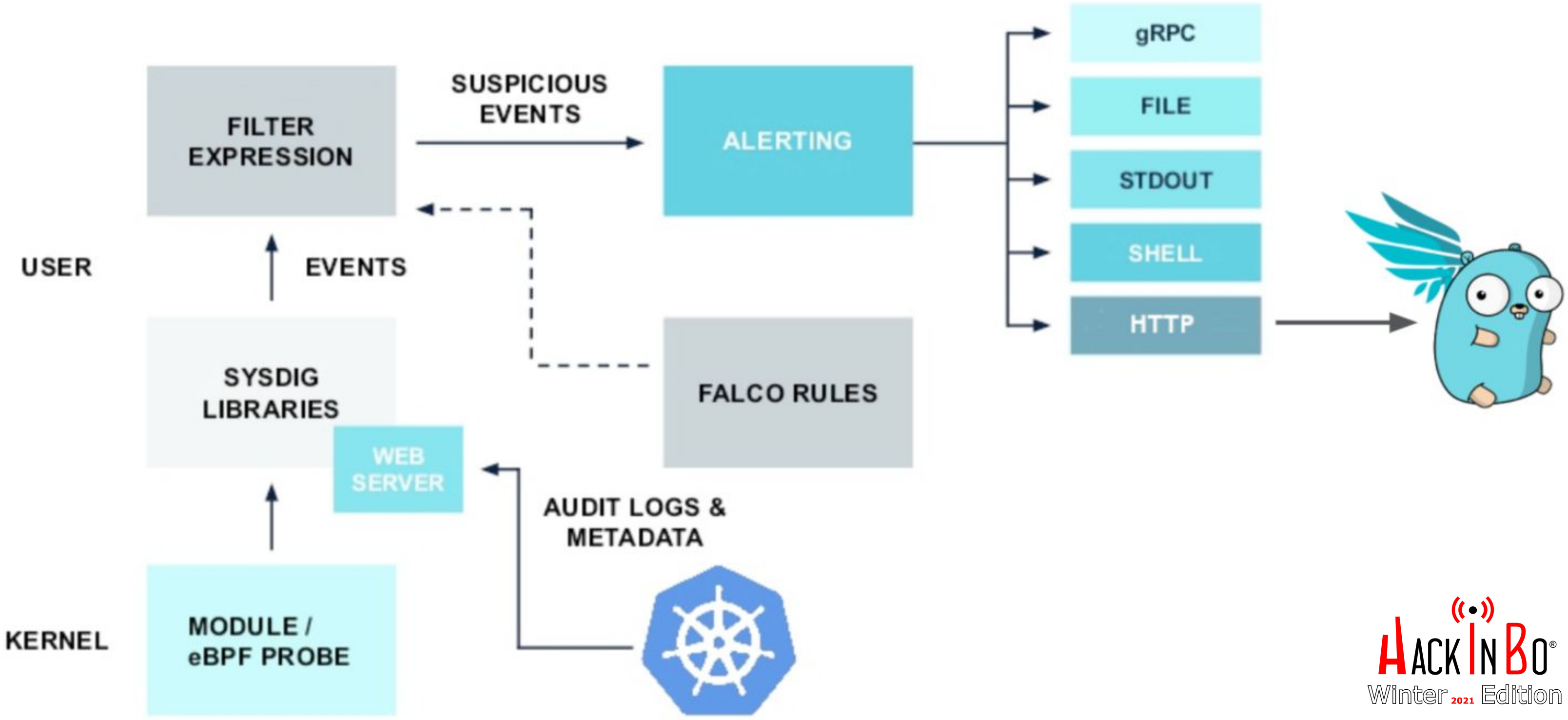
Falco Rules



Falco MITRE Rule Matrix

Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Exfiltration
DB program spawned process	Modify Shell Configuration File	Launch Privileged Container	Clear Log Activities	Read sensitive file trusted after startup	Read Shell Configuration File	Launch Privileged Container	System procs network activity
Run shell untrusted	Schedule Cron Jobs	Non sudo setuid	Delete Bash History	Read sensitive file untrusted	Read ssh information	Launch Sensitive Mount Container	Interpreted procs inbound network
Terminal shell in container	Update Package Repository			Search Private Keys or Passwords	Read sensitive file untrusted	Launch Disallowed Container	Interpreted procs outbound network
Netcat Remote Code Execution in Container	Write below binary dir Write below monitored dir				Contact K8S API Server From Container		Unexpected UDP Traffic
	Write below etc Write below root Write below rpm database				Launch Suspicious Network Tool in Container		Launch Suspicious Network Tool in Container
	Modify binary dirs Mkdir binary dirs				Launch Suspicious Network Tool on Host		Launch Suspicious Network Tool on Host
	User mgmt binaries						
	Create files below dev						
	Launch Package Management Process in Container						
	Remove Bulk Data from Disk Set						
	Create Hidden Files or Directories						
	Setuid or Setgid bit						

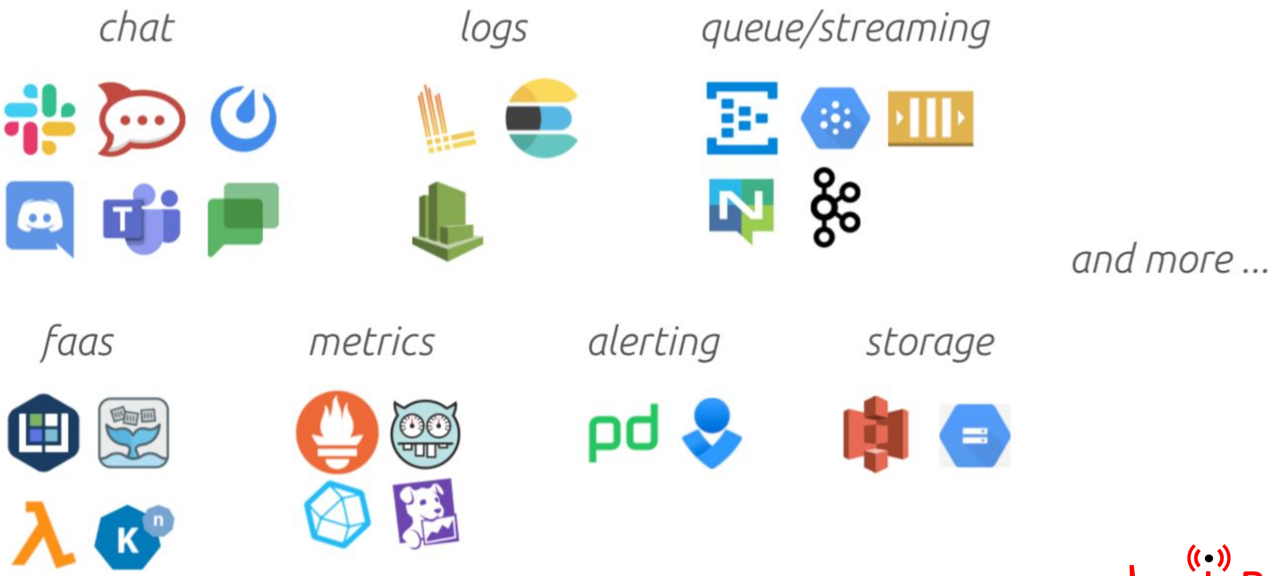
#Falco + Falcosidekick



Hack In Bo® Winter 2021 Edition
17ª EDIZIONE

#Falcosidekick

Connects Falco to your ecosystem



chat

logs

queue/streaming

and more ...

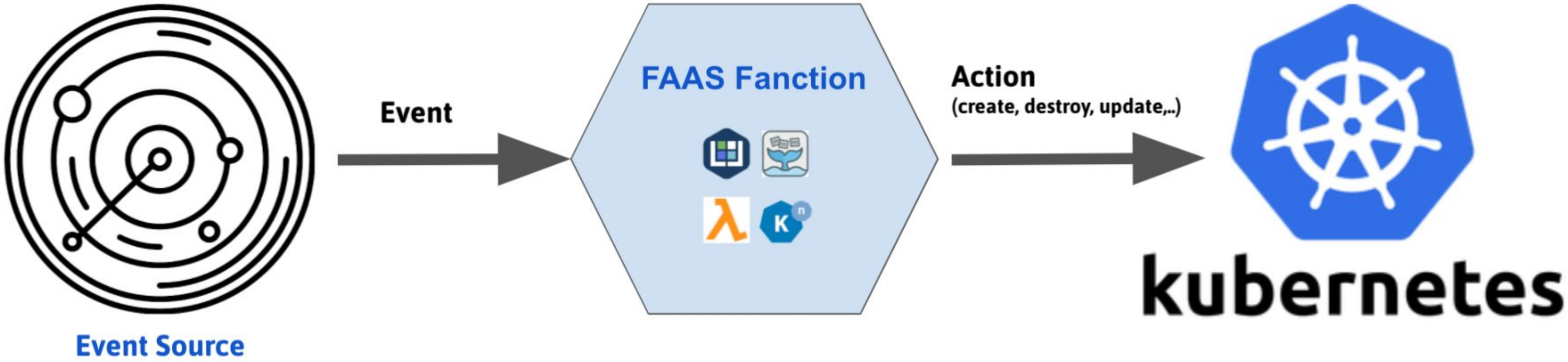
faas

metrics

alerting

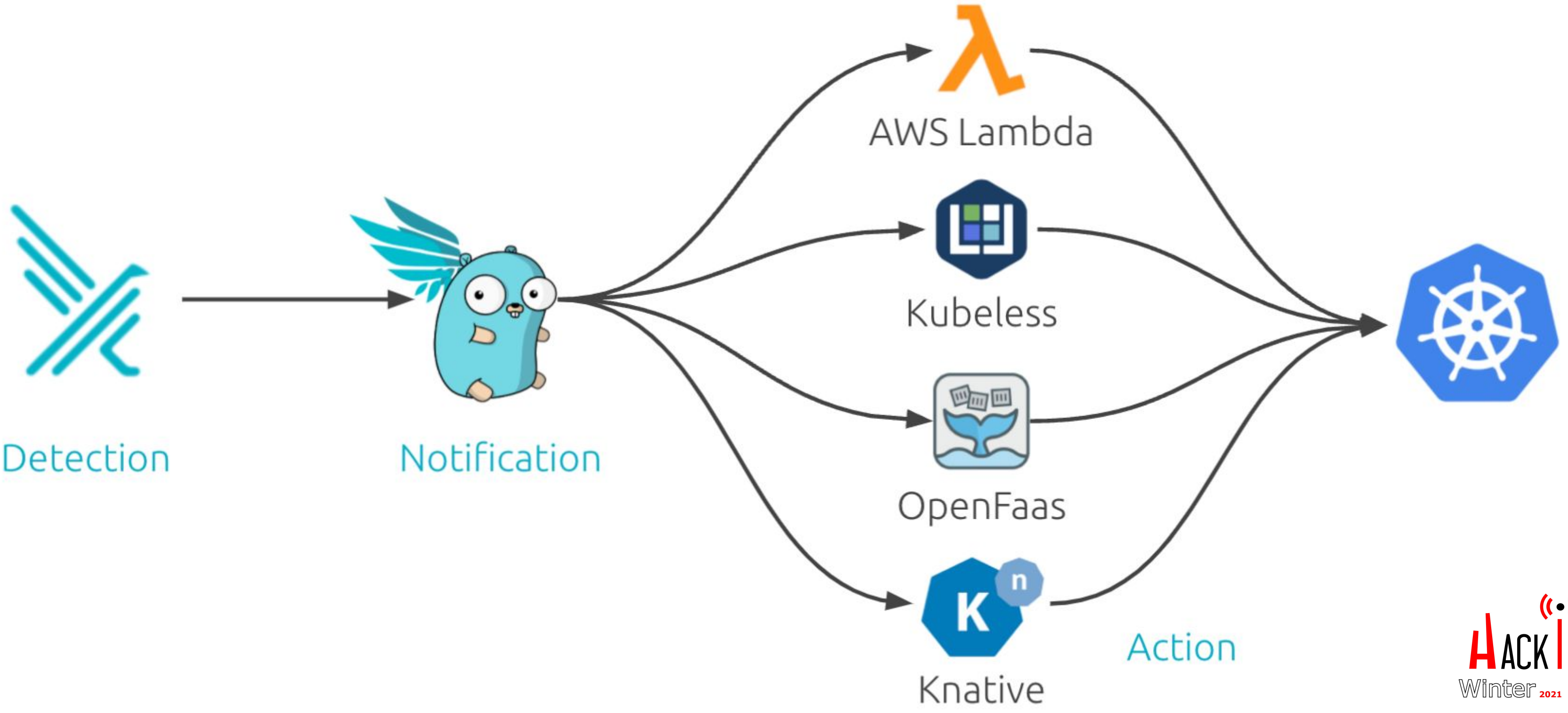
storage

The FaaS Power



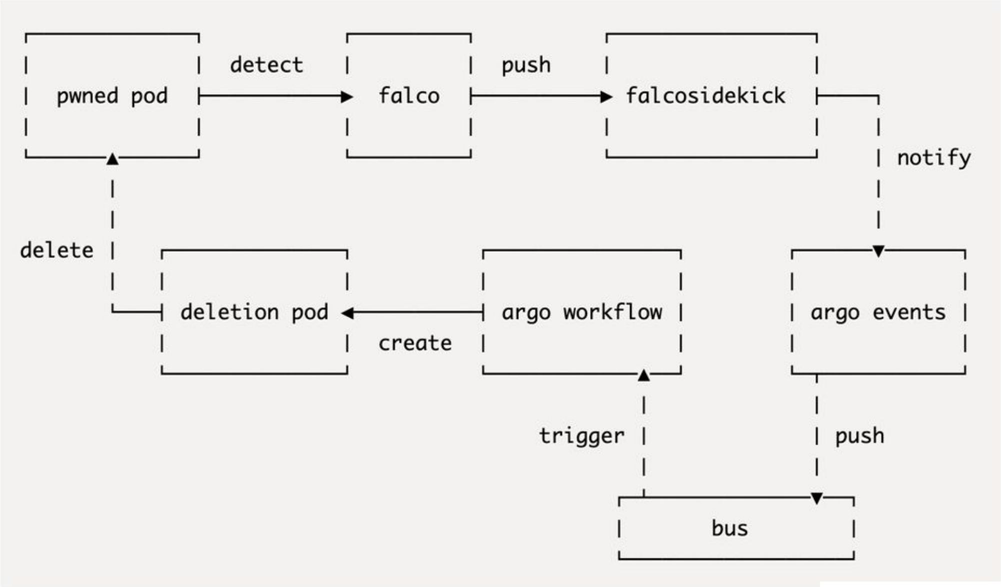
WAIT A MINUTE
quickmeme.com

#Falco + Falcosidekick = A K8s Response Engine



K8s Response Engine using Argo - Demo

- **Falco - https://github.com/falcosecurity/falco**
- **Falcosidekick - https://github.com/falcosecurity/falcosidekick**
- **Argo Events - https://github.com/argoproj/argo-events**
- **Argo Workflow - https://github.com/argoproj/argo-workflows**



pwned pod

detect

falco

push

falcosidekick

notify

argo events

push

bus

trigger

argo workflow

create

deletion pod

delete

Demo

Contribute to Falco!

- Get Started with Falco.org
- Checkout the Falco Project in GitHub
- Meet the maintainers on the Falco Slack
- Follow the @falco_org on Twitter

Q&A