

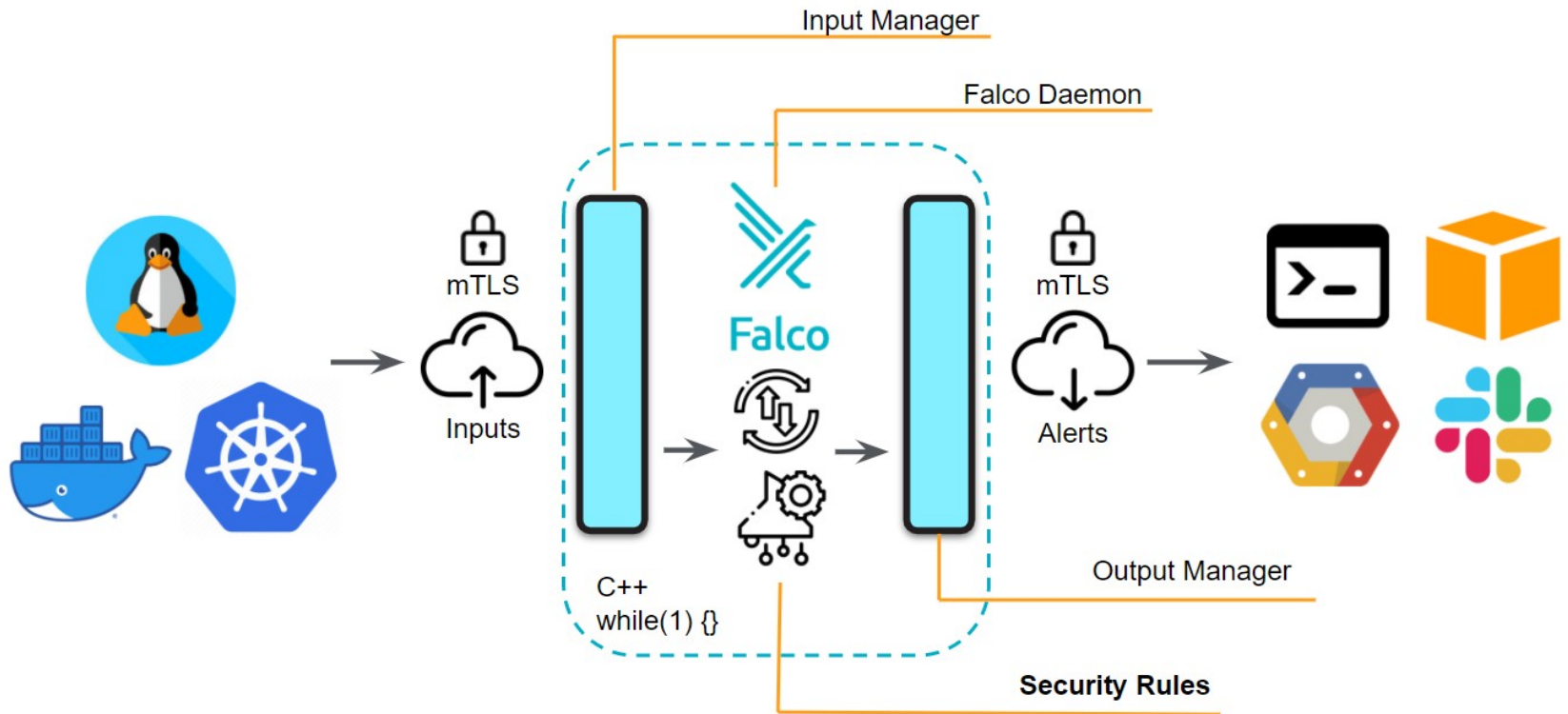


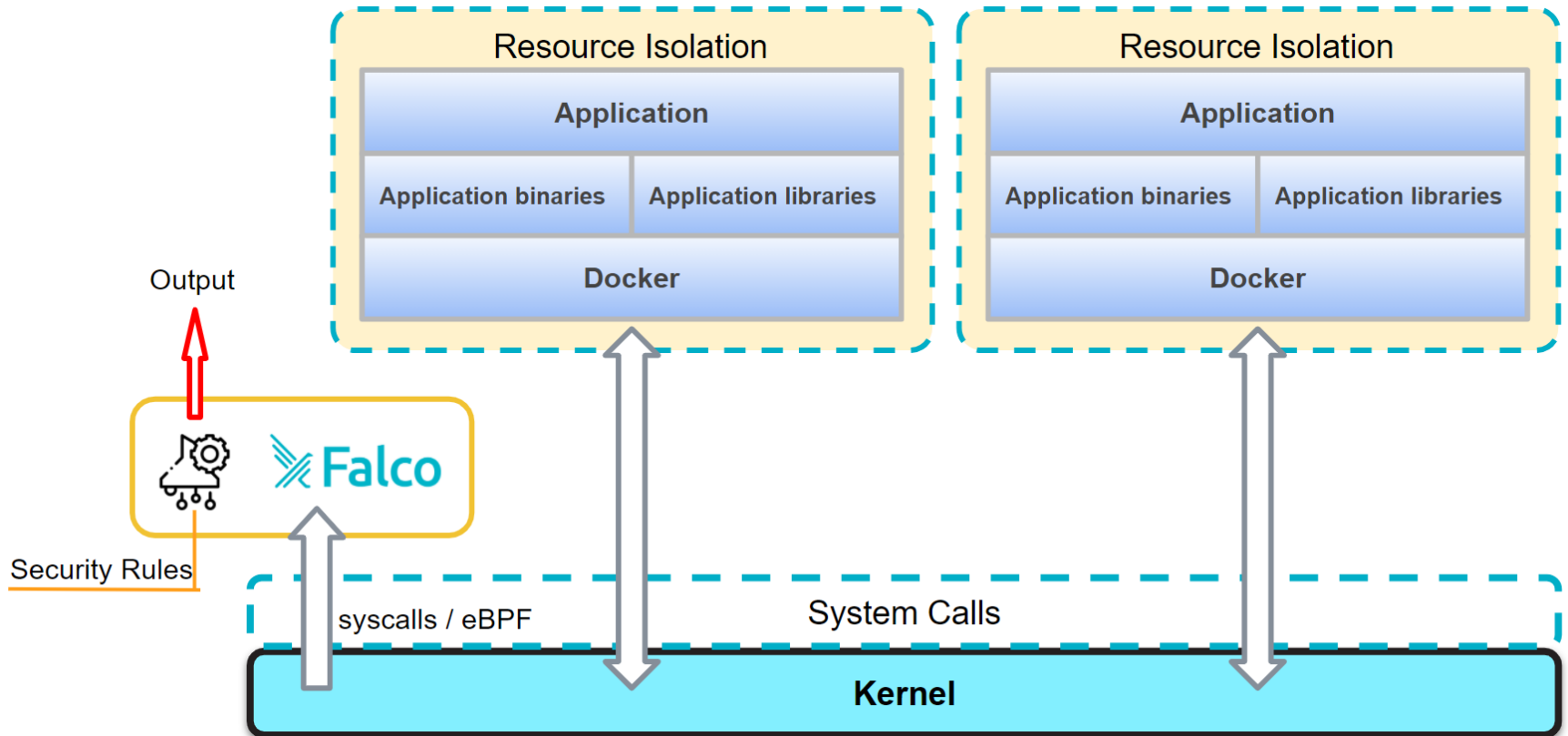
Falco para seguridad en kernel de host y contenedores



Operativa de Falco en Kernel

Arquitectura







Instalación directa en host

Prerequisitos para practicar

- Vagrant : www.vagrantup.com
- Virtual Box : www.virtualbox.org
- Git : git-scm.com

Repositorio con MV Vagrant con ejemplos de uso de Falco:
<https://github.com/sysdiglabs/falco-workshop>

```
git clone git@github.com:sysdiglabs/falco-workshop.git
```

Instalación Debian

```
$ sudo apt-get update
$ sudo apt-get -y install gpg curl
$ curl -o install-falco.sh -s \
  https://s3.amazonaws.com/download.draios.com/stable/install-falco
```

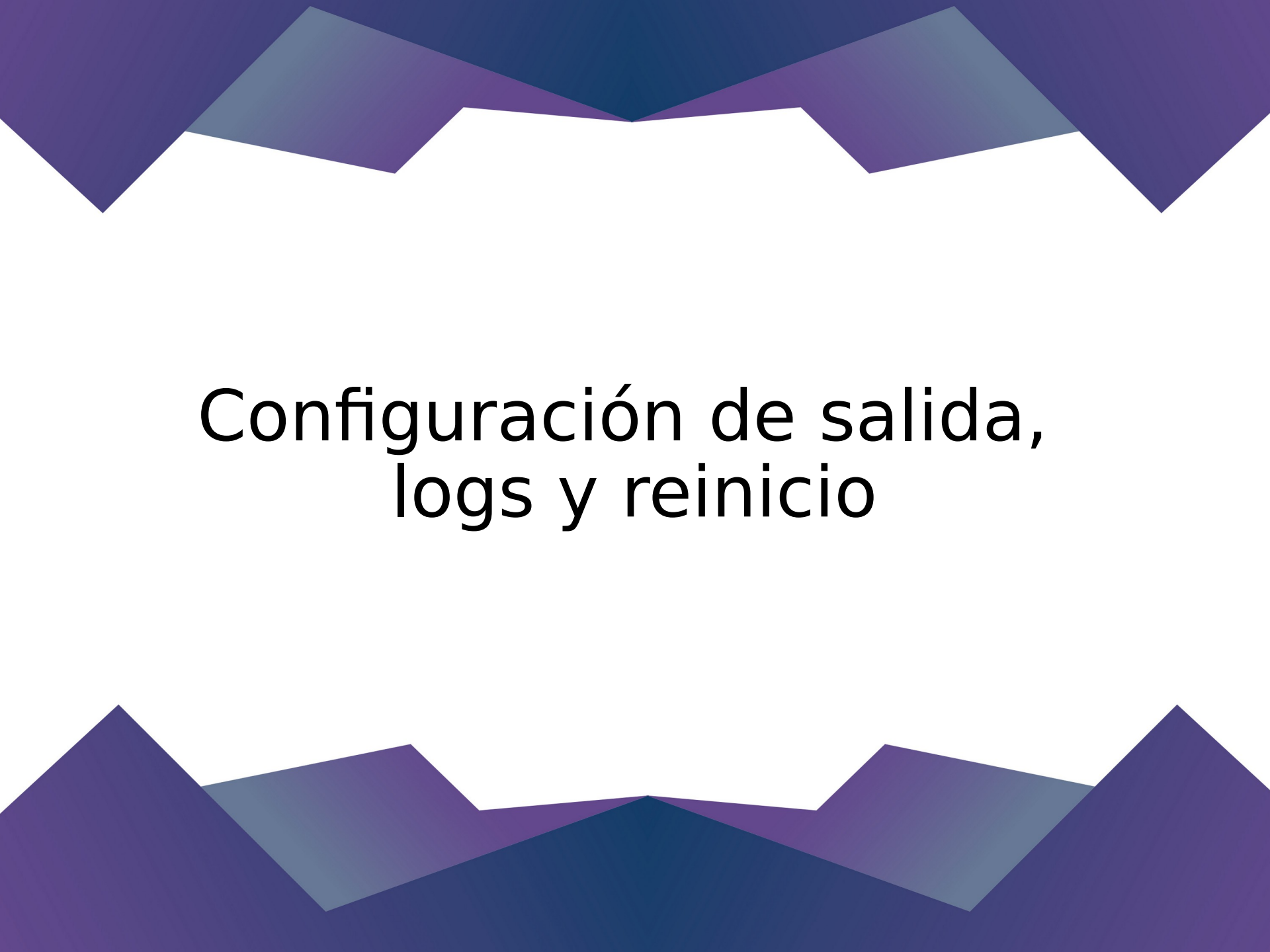
```
$ sudo bash install-falco.sh
```

```
# install-falco.sh *equivalent* instructions (sudo):
$ curl -s https://s3.amazonaws.com/download.draios.com/DRAIOS-GPG-KEY.public |
\
  apt-key add -
$ curl -s -o /etc/apt/sources.list.d/draios.list \
  https://s3.amazonaws.com/download.draios.com/stable/deb/draios.list
$ apt-get update
$ apt-get -y install linux-headers-$(uname -r)
$ apt-get install -y falco
```

Instalación en host mediante Docker

Requiere Kernel de linux compatible

```
$ sudo apt-get -y install linux-headers-$(uname -r)
$ docker pull falcosecurity/falco
$ docker run -i -t --name falco --privileged \
  -v /var/run/docker.sock:/host/var/run/docker.sock \
  -v /dev:/host/dev \
  -v /proc:/host/proc:ro \
  -v /boot:/host/boot:ro \
  -v /lib/modules:/host/lib/modules:ro \
  -v /usr:/host/usr:ro \
  falcosecurity/falco
```

Configuración de salida, logs y reinicio

```
$ sudo touch /var/log/falco_events.log  
$ sudo nano /etc/falco/falco.yaml
```

Cambiar:

```
file_output:  
  enabled: true  
  keep_alive: true  
  filename: /var/log/falco_events.log
```

Reiniciar servicio:

```
$ sudo /etc/init.d/falco restart
```

Output targets:

- ➔ file_output (log file)
- ➔ gRPC
- ➔ HTTP output (POST)
- ➔ syslog output

Cómo probar que Falco funciona

```
$ su
$ sudo echo "hello" > /var/log/falco_events.log
$ exit
$ cat /var/log/falco_events.log
```

```
6:15:59.922240449: Warning Log files were tampered
(user=root command=bash file=/var/log/falco_events.log
container_id=host image=<NA>)
```