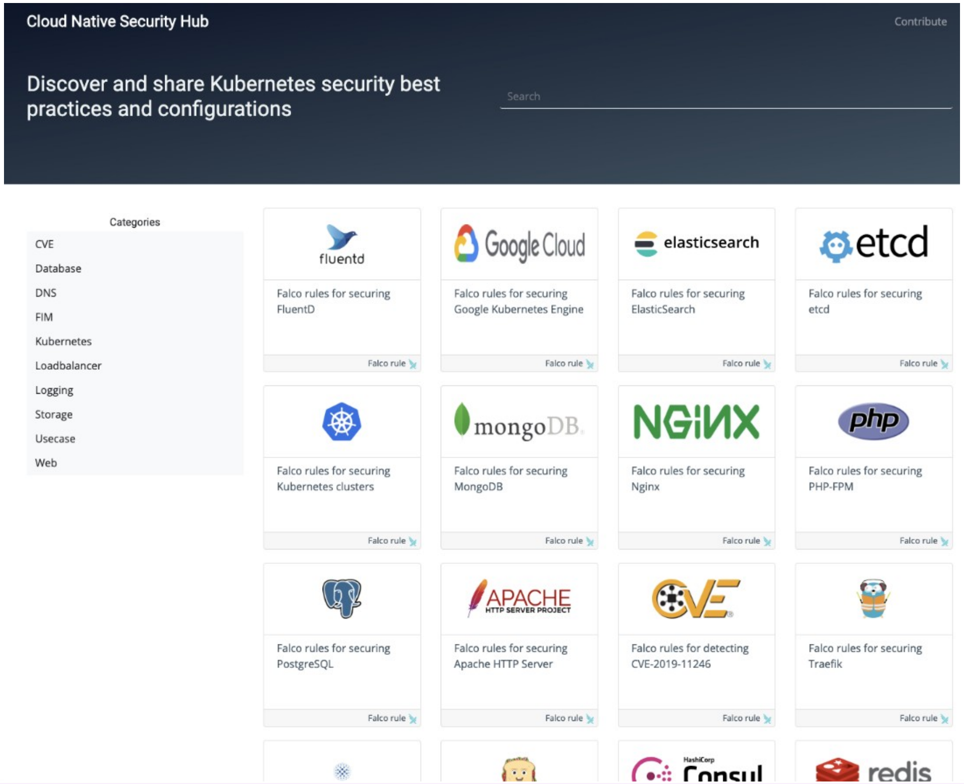
Utilidades adicionales para Falco

Falco: Utilidades adicionales, webs y artículos de referencia, demo uso con Docker

Cloud Native Security Hub

- https://securityhub.dev



Cloud Native Security Hub

Contribute

Discover and share Kubernetes security best practices and configurations

Search

Categories

- CVE
- Database
- DNS
- FIM
- Kubernetes
- Loadbalancer
- Logging
- Storage
- Usecase
- Web

Falco rules for securing FluentD — Falco rule

Falco rules for securing Google Kubernetes Engine — Falco rule

Falco rules for securing ElasticSearch — Falco rule

Falco rules for securing etcd — Falco rule

Falco rules for securing Kubernetes clusters — Falco rule

Falco rules for securing MongoDB — Falco rule

Falco rules for securing Nginx — Falco rule

Falco rules for securing PHP-FPM — Falco rule

Falco rules for securing PostgreSQL — Falco rule

Falco rules for securing Apache HTTP Server — Falco rule

Falco rules for detecting CVE-2019-11246 — Falco rule

Falco rules for securing Traefik — Falco rule

Utilidades más interesantes

- **Kubernetes Response Engine**
  Send events to serverless functions to execute playbooks
  https://github.com/falcosecurity/kubernetes-response-engine
- **Falco Sidekick**
  Send events to other targets as Slack, PagerDuty, etc.
  https://github.com/falcosecurity/falcosidekick
- **Event generator**
  Binary that executes commands that Falco rules should detect
  https://falco.org/docs/event-sources/sample-events/

Ejemplo: Instalar Falco con Docker

```
# Instalar driver de Kernel

docker pull falcosecurity/falco-driver-loader:latest

docker run --rm -i -t \
    --privileged \
    -v /root/.falco:/root/.falco \
    -v /proc:/host/proc:ro \
    -v /boot:/host/boot:ro \
    -v /lib/modules:/host/lib/modules:ro \
    -v /usr:/host/usr:ro \
    -v /etc:/host/etc:ro \
    falcosecurity/falco-driver-loader:latest
```

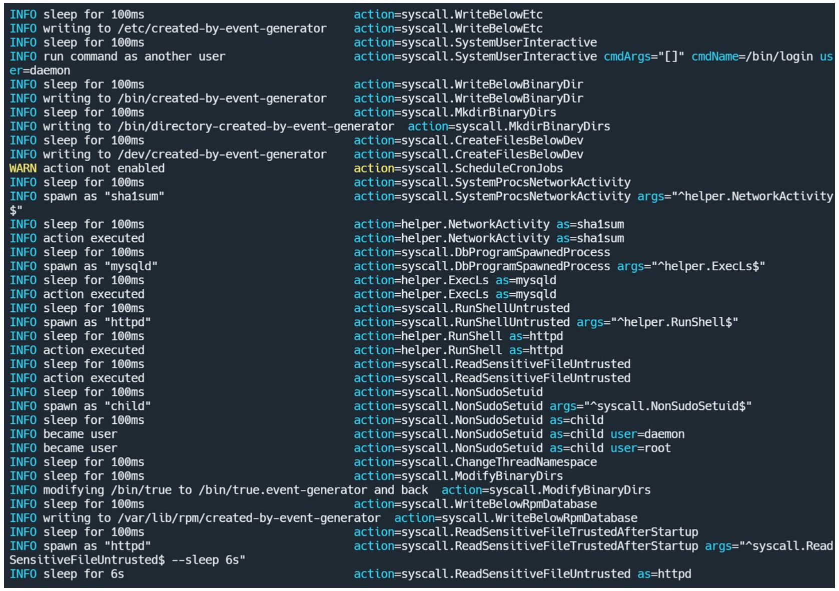
```
# Ejecutar Falco con privilegios

docker pull falcosecurity/falco:latest

docker run --rm -i -t \
    --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 \
    -v /etc:/host/etc:ro \
    falcosecurity/falco:latest
```

Ejemplo: Ejecutar event generator

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



```
INFO sleep for 100ms                               action=syscall.WriteBelowEtc
INFO writing to /etc/created-by-event-generator    action=syscall.WriteBelowEtc
INFO sleep for 100ms                               action=syscall.SystemUserInteractive
INFO run command as another user                   action=syscall.SystemUserInteractive cmdArgs="[]" cmdName=/bin/login us
er=daemon
INFO sleep for 100ms                               action=syscall.WriteBelowBinaryDir
INFO writing to /bin/created-by-event-generator    action=syscall.WriteBelowBinaryDir
INFO sleep for 100ms                               action=syscall.MkdirBinaryDirs
INFO writing to /bin/directory-created-by-event-generator  action=syscall.MkdirBinaryDirs
INFO sleep for 100ms                               action=syscall.CreateFilesBelowDev
INFO writing to /dev/created-by-event-generator    action=syscall.CreateFilesBelowDev
WARN action not enabled                            action=syscall.ScheduleCronJobs
INFO sleep for 100ms                               action=syscall.SystemProcsNetworkActivity
INFO spawn as "sha1sum"                            action=syscall.SystemProcsNetworkActivity args="^helper.NetworkActivity
$"
INFO sleep for 100ms                               action=helper.NetworkActivity as=sha1sum
INFO action executed                               action=helper.NetworkActivity as=sha1sum
INFO sleep for 100ms                               action=syscall.DbProgramSpawnedProcess
INFO spawn as "mysqld"                             action=syscall.DbProgramSpawnedProcess args="^helper.ExecLs$"
INFO sleep for 100ms                               action=helper.ExecLs as=mysqld
INFO action executed                               action=helper.ExecLs as=mysqld
INFO sleep for 100ms                               action=syscall.RunShellUntrusted
INFO spawn as "httpd"                              action=syscall.RunShellUntrusted args="^helper.RunShell$"
INFO sleep for 100ms                               action=helper.RunShell as=httpd
INFO action executed                               action=helper.RunShell as=httpd
INFO sleep for 100ms                               action=syscall.ReadSensitiveFileUntrusted
INFO action executed                               action=syscall.ReadSensitiveFileUntrusted
INFO sleep for 100ms                               action=syscall.NonSudoSetuid
INFO spawn as "child"                              action=syscall.NonSudoSetuid args="^syscall.NonSudoSetuid$"
INFO sleep for 100ms                               action=syscall.NonSudoSetuid as=child
INFO became user                                   action=syscall.NonSudoSetuid as=child user=daemon
INFO became user                                   action=syscall.NonSudoSetuid as=child user=root
INFO sleep for 100ms                               action=syscall.ChangeThreadNamespace
INFO sleep for 100ms                               action=syscall.ModifyBinaryDirs
INFO modifying /bin/true to /bin/true.event-generator and back  action=syscall.ModifyBinaryDirs
INFO sleep for 100ms                               action=syscall.WriteBelowRpmDatabase
INFO writing to /var/lib/rpm/created-by-event-generator  action=syscall.WriteBelowRpmDatabase
INFO sleep for 100ms                               action=syscall.ReadSensitiveFileTrustedAfterStartup
INFO spawn as "httpd"                              action=syscall.ReadSensitiveFileTrustedAfterStartup args="^syscall.Read
SensitiveFileUntrusted$ --sleep 6s"
INFO sleep for 6s                                  action=syscall.ReadSensitiveFileUntrusted as=httpd
```

Utilidades nicho

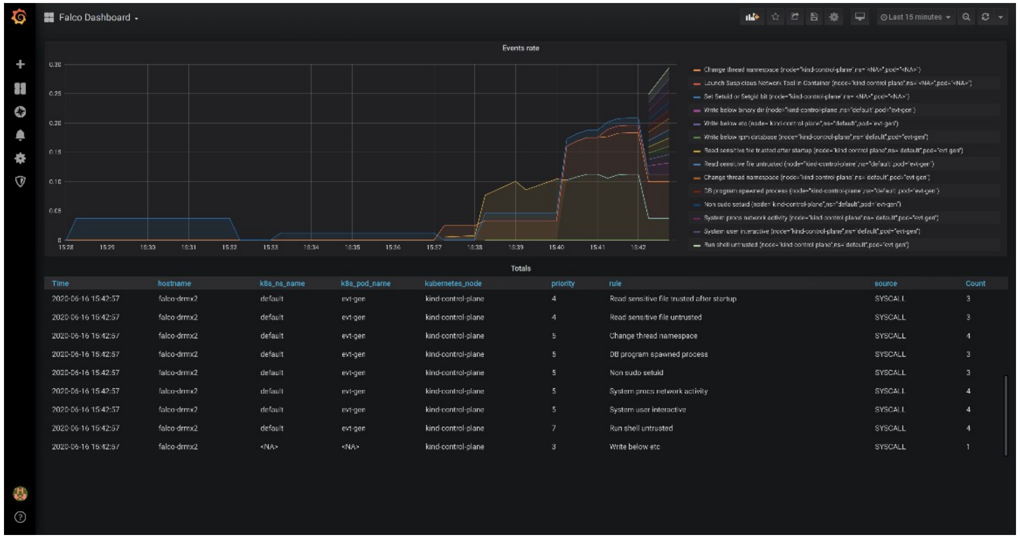
- **Falco Prometheus Exporter**
  Prometheus metrics for Falco security events
  https://github.com/falcosecurity/falco-exporter

- **Falco PSP Convert**
  Convert PSP to Falco rules to test them before enforcing
  https://falco.org/docs/psp-support/

Blog de Falco

- Falco on Kind with Prometheus and Grafana https://falco.org/blog/falco-kind-prometheus-grafana/

- Detect CVE-2020-8557 using Falco https://falco.org/blog/detect-cve-2020-8557/


Falco Dashboard
Last 15 minutes
Events rate
0.30
0.25
0.20
0.15
0.10
0.05
0
15:28
15:29
15:30
15:31
15:32
15:33
15:34
15:35
15:36
15:37
15:38
15:39
15:40
15:41
15:42
Change thread namespace (node="kind-control-plane",ns="<NA>",pod="<NA>")
Launch Suspicious Network Tool in Container (node="kind control plane",ns="<NA>",pod="<NA>")
Set Setuid or Setgid bit (node="kind-control-plane",ns="<NA>",pod="<NA>")
Write below binary dir (node="kind-control-plane",ns="default",pod="evt-gen")
Write below etc (node="kind-control-plane",ns="default",pod="evt-gen")
Write below rpm database (node="kind-control-plane",ns="default",pod="evt-gen")
Read sensitive file trusted after startup (node="kind control plane",ns="default",pod="evt gen")
Read sensitive file untrusted (node="kind-control-plane",ns="default",pod="evt-gen")
Change thread namespace (node="kind control plane",ns="default",pod="evt-gen")
DB program spawned process (node="kind-control-plane",ns="default",pod="evt-gen")
Non sudo setuid (node="kind-control-plane",ns="default",pod="evt-gen")
System procs network activity (node="kind-control-plane",ns="default",pod="evt-gen")
System user interactive (node="kind-control-plane",ns="default",pod="evt-gen")
Run shell untrusted (node="kind control plane",ns="default",pod="evt gen")

Totals

Time	hostname	k8s_ns_name	k8s_pod_name	kubernetes_node	priority	rule	source	Count
2020-06-16 15:42:57	falco-drmx2	default	evt-gen	kind-control-plane	4	Read sensitive file trusted after startup	SYSCALL	3
2020-06-16 15:42:57	falco-drmx2	default	evt-gen	kind-control-plane	4	Read sensitive file untrusted	SYSCALL	3
2020-06-16 15:42:57	falco-drmx2	default	evt-gen	kind-control-plane	5	Change thread namespace	SYSCALL	4
2020-06-16 15:42:57	falco-drmx2	default	evt-gen	kind-control-plane	5	DB program spawned process	SYSCALL	3
2020-06-16 15:42:57	falco-drmx2	default	evt-gen	kind-control-plane	5	Non sudo setuid	SYSCALL	3
2020-06-16 15:42:57	falco-drmx2	default	evt-gen	kind-control-plane	5	System procs network activity	SYSCALL	4
2020-06-16 15:42:57	falco-drmx2	default	evt-gen	kind-control-plane	5	System user interactive	SYSCALL	4
2020-06-16 15:42:57	falco-drmx2	default	evt-gen	kind-control-plane	7	Run shell untrusted	SYSCALL	4
2020-06-16 15:42:57	falco-drmx2	<NA>	<NA>	kind-control-plane	3	Write below etc	SYSCALL	1

Artículos externos sobre Falco

- Shopify, enforcing runtime security with Falco
  Upcoming talk at Kubecon 2020
  https://events.linuxfoundation.org/kubecon-cloudnativecon-europe/
- Runtime Security in Rancher with Falco
  https://rancher.com/blog/2020/runtime-security-with-falco/

Artículos de Sysdig sobre Falco

- MITRE ATT&CK framework for container runtime security with Falco https://sysdig.com/blog/mitre-attck-framework-for-container-runtime-security-with-sysdig-falco/
- Protection From Malicious Python Libraries Jeilyfish and Python3-dateutil https://sysdig.com/blog/malicious-python-libraries-jeilyfish-dateutil/
- SELinux, Seccomp, Falco, and you: A technical discussion https://sysdig.com/blog/selinux-seccomp-falco-technical-discussion/