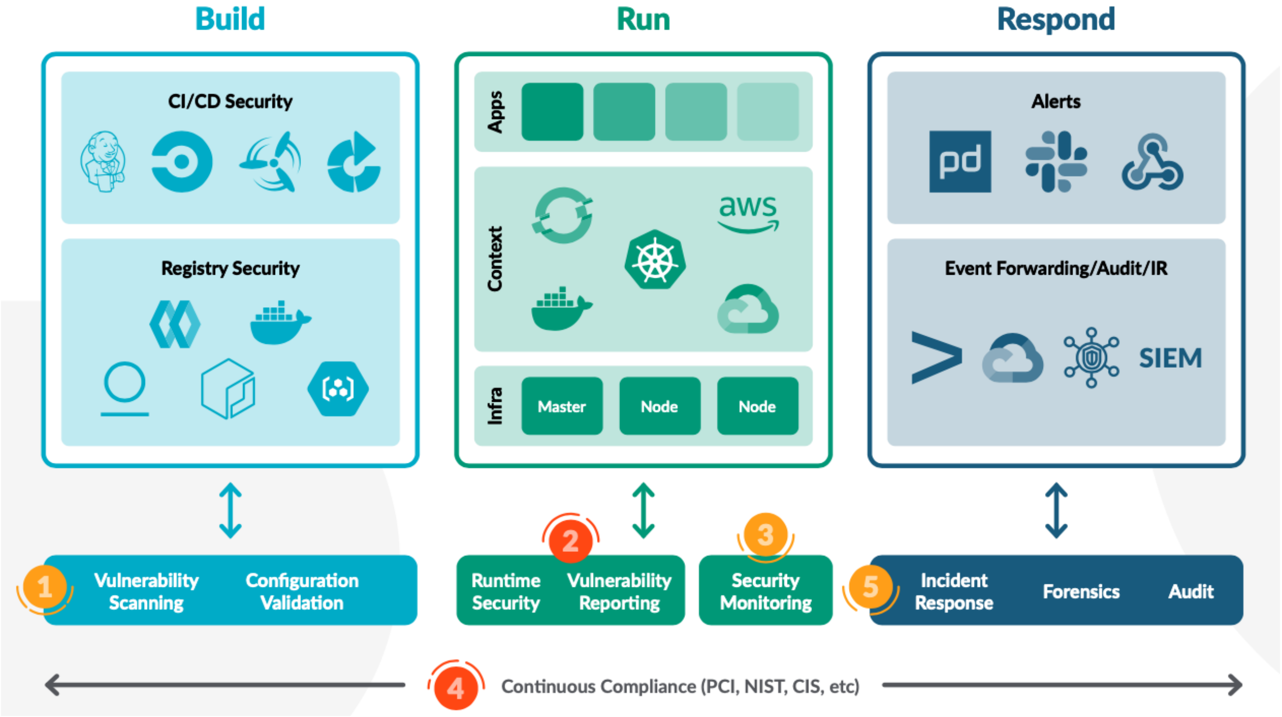
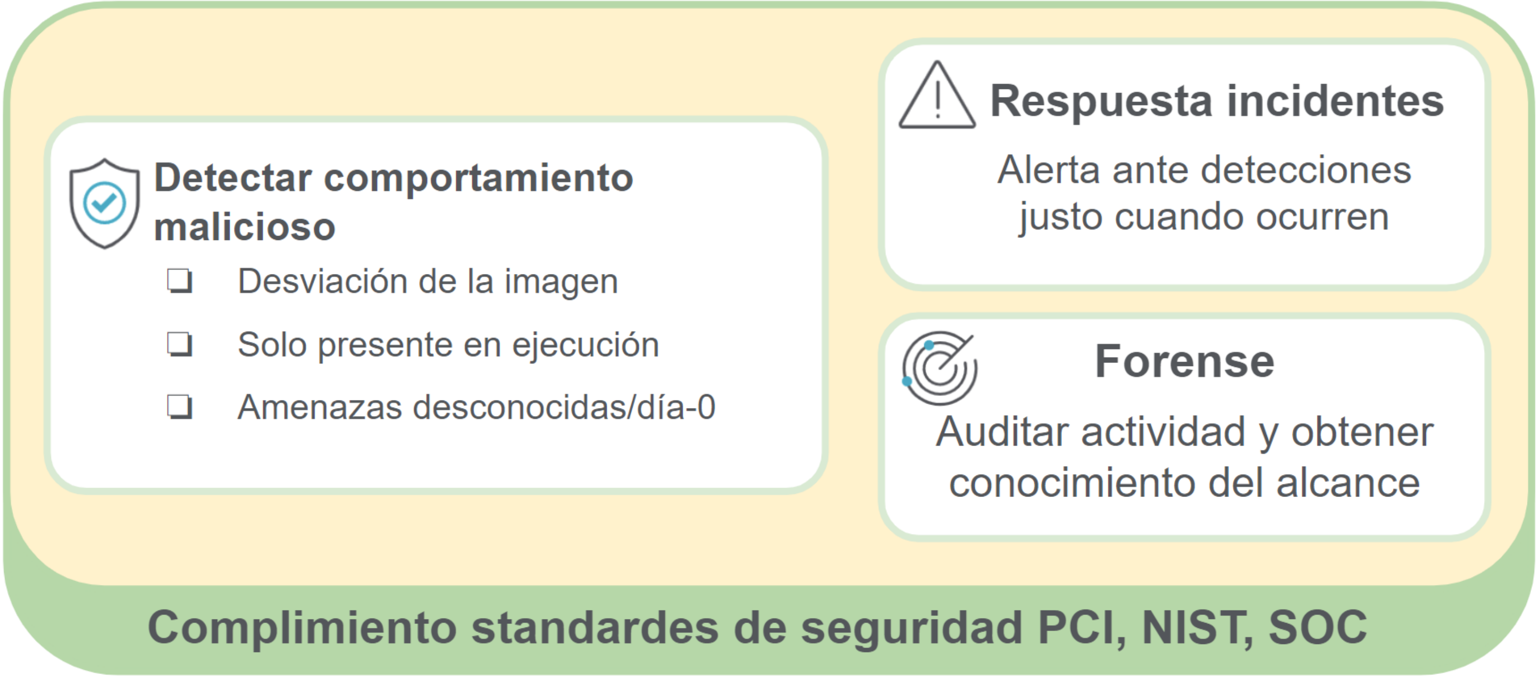
Runtime Security e introducción a Falco

Runtime security en el ciclo DevOps



¿Por qué *runtime security*?



Detectar comportamiento malicioso

- ❑ Desviación de la imagen
- ❑ Solo presente en ejecución
- ❑ Amenazas desconocidas/día-0

Respuesta incidentes

Alerta ante detecciones justo cuando ocurren

Forense

Auditar actividad y obtener conocimiento del alcance

Complimiento standardes de seguridad PCI, NIST, SOC

Falco

Proyecto software libre de la Cloud Native Computing Foundation

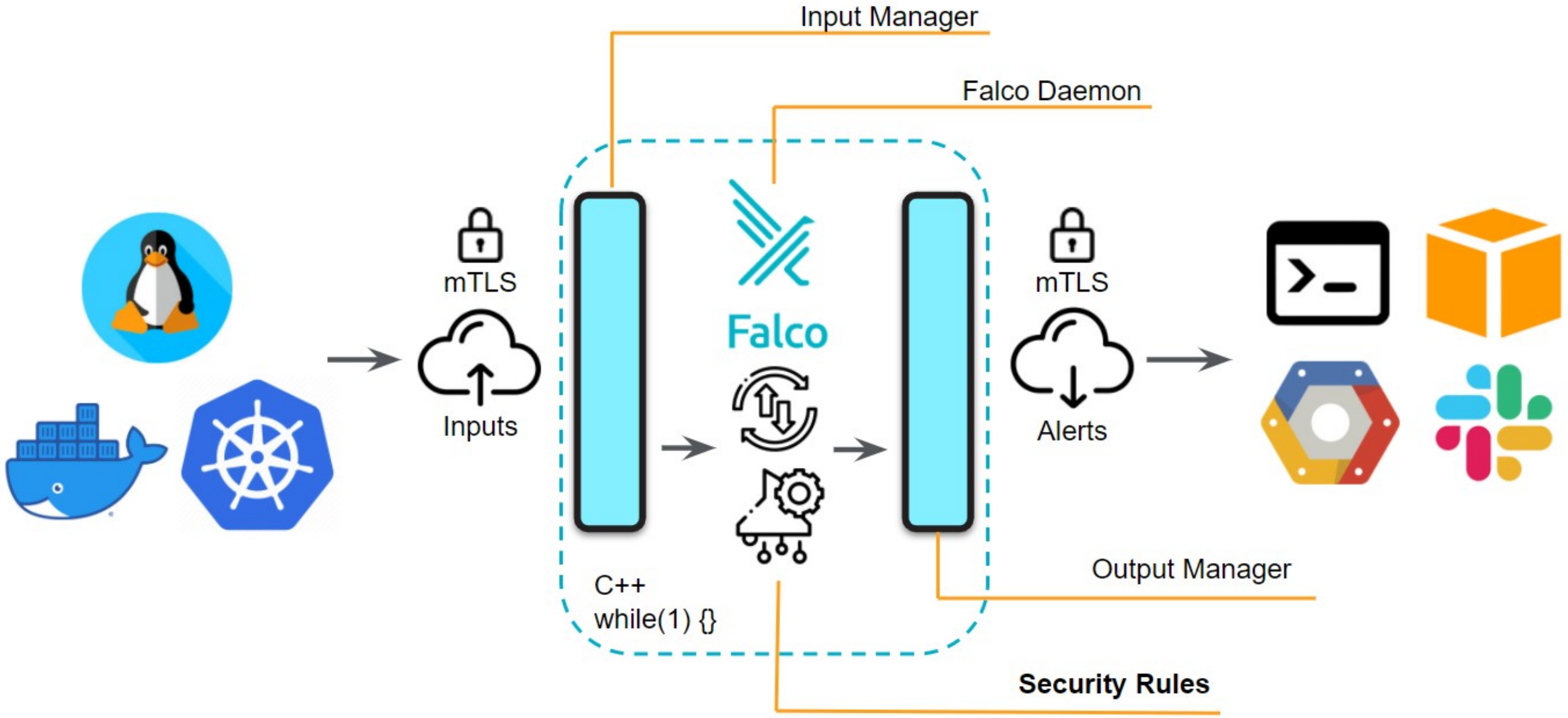
falco.org | landscape.cncf.io/selected=falco

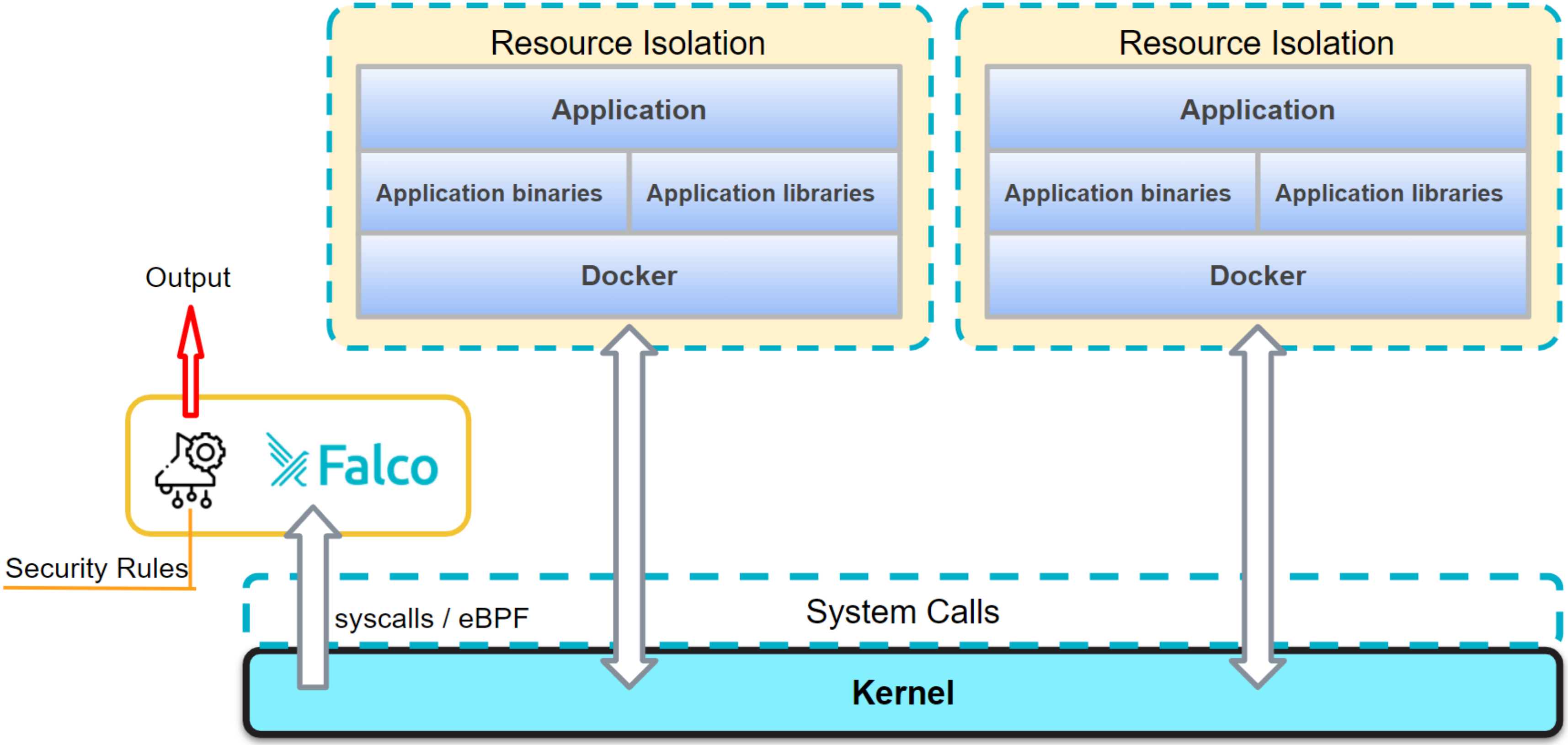
CLOUD NATIVE COMPUTING FOUNDATION

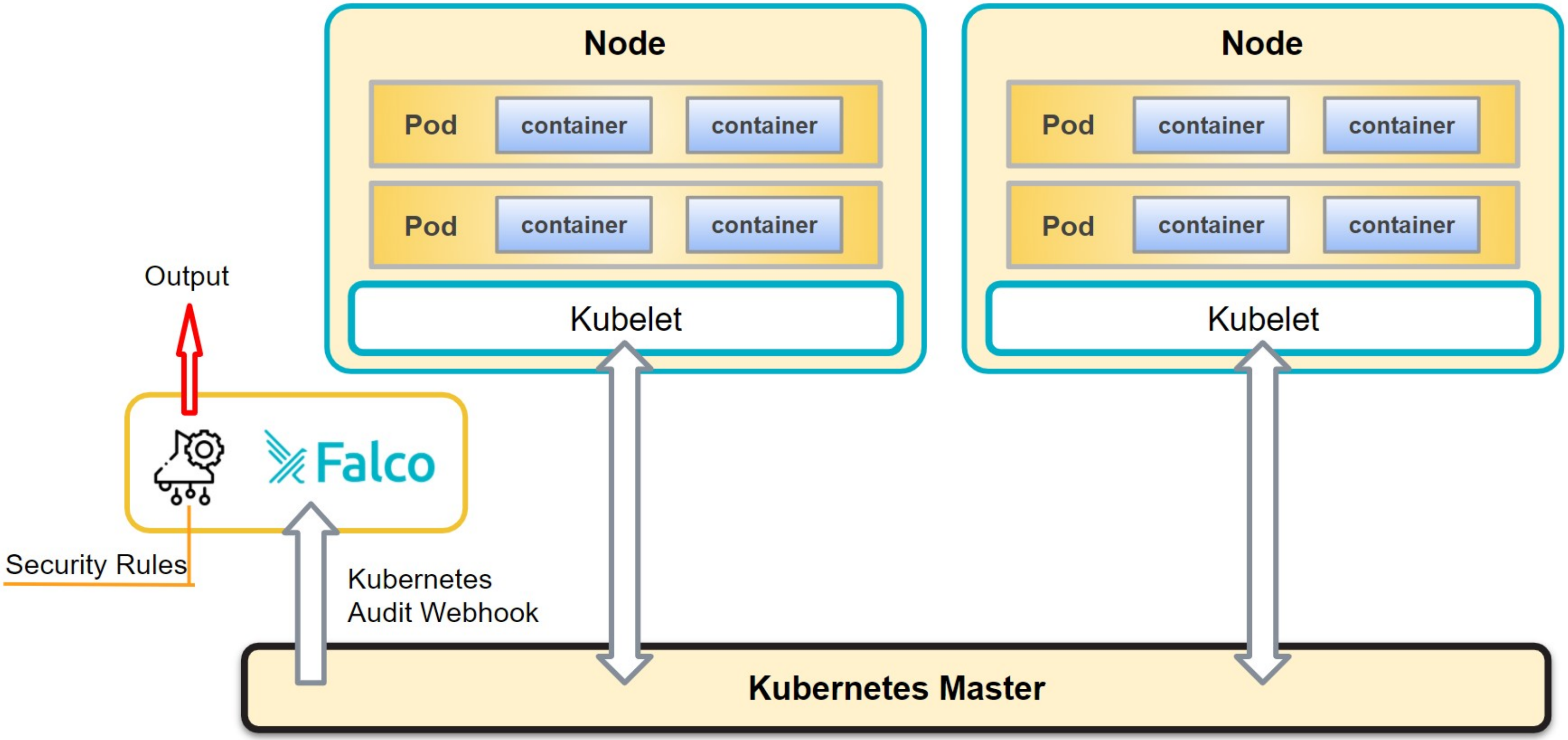
kubernetes

THE LINUX FOUNDATION

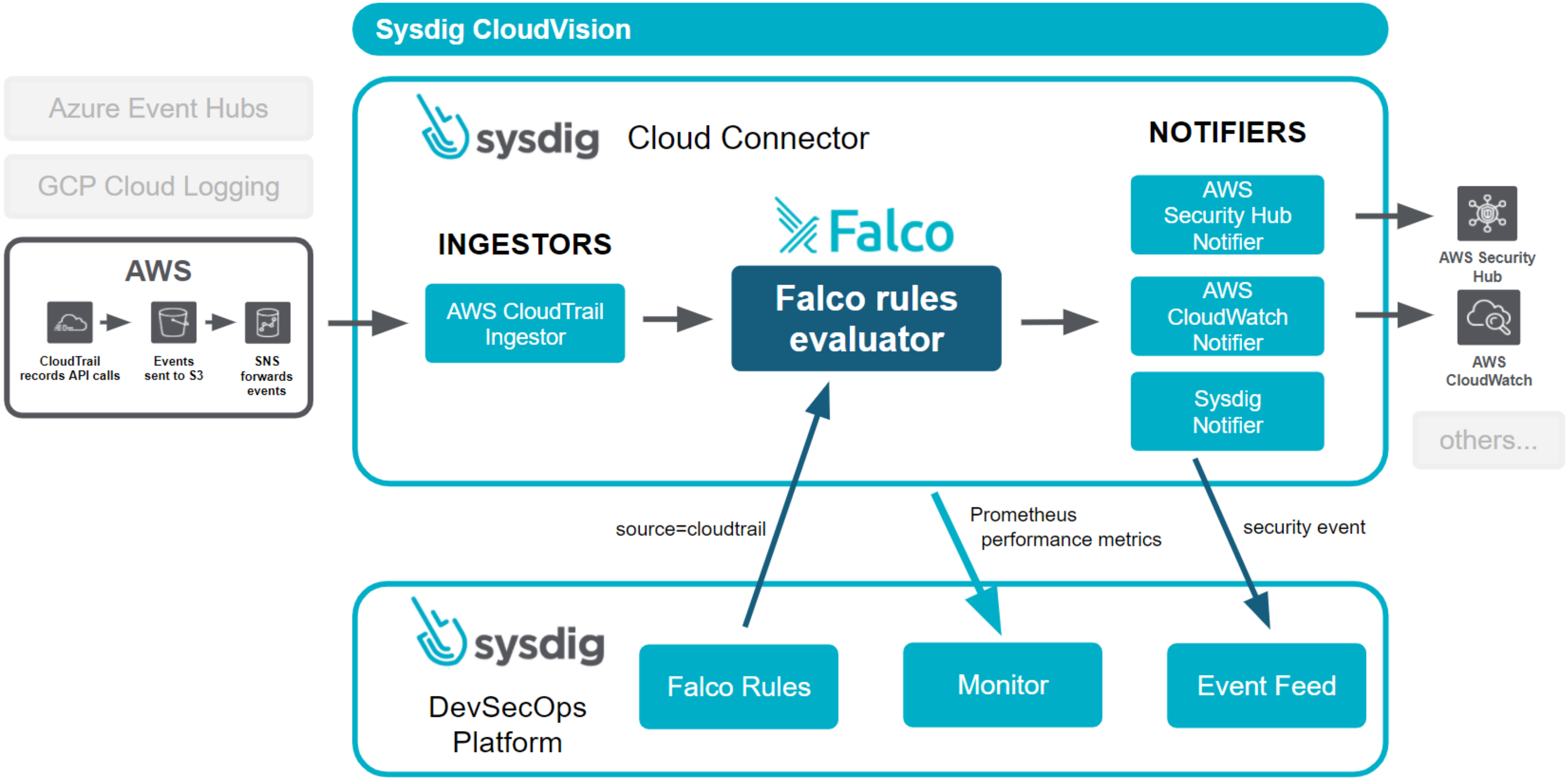
Arquitectura




Resource Isolation
Application
Application binaries
Application libraries
Docker
Resource Isolation
Application
Application binaries
Application libraries
Docker
Output
Falco
Security Rules
syscalls / eBPF
System Calls
Kernel


Node
Pod
container
container
Pod
container
container
Kubelet
Node
Pod
container
container
Pod
container
container
Kubelet
Output
Falco
Security Rules
Kubernetes
Audit Webhook
Kubernetes Master

QUANTIKA 14


Sysdig CloudVision
Azure Event Hubs
GCP Cloud Logging
AWS
CloudTrail records API calls
Events sent to S3
SNS forwards events
sysdig Cloud Connector
INGESTORS
AWS CloudTrail Ingestor
Falco
Falco rules evaluator
NOTIFIERS
AWS Security Hub Notifier
AWS CloudWatch Notifier
Sysdig Notifier
AWS Security Hub
AWS CloudWatch
others...
source=cloudtrail
Prometheus performance metrics
security event
sysdig DevSecOps Platform
Falco Rules
Monitor
Event Feed

falco.org

Sitio principal:

falco.org

Documentación:

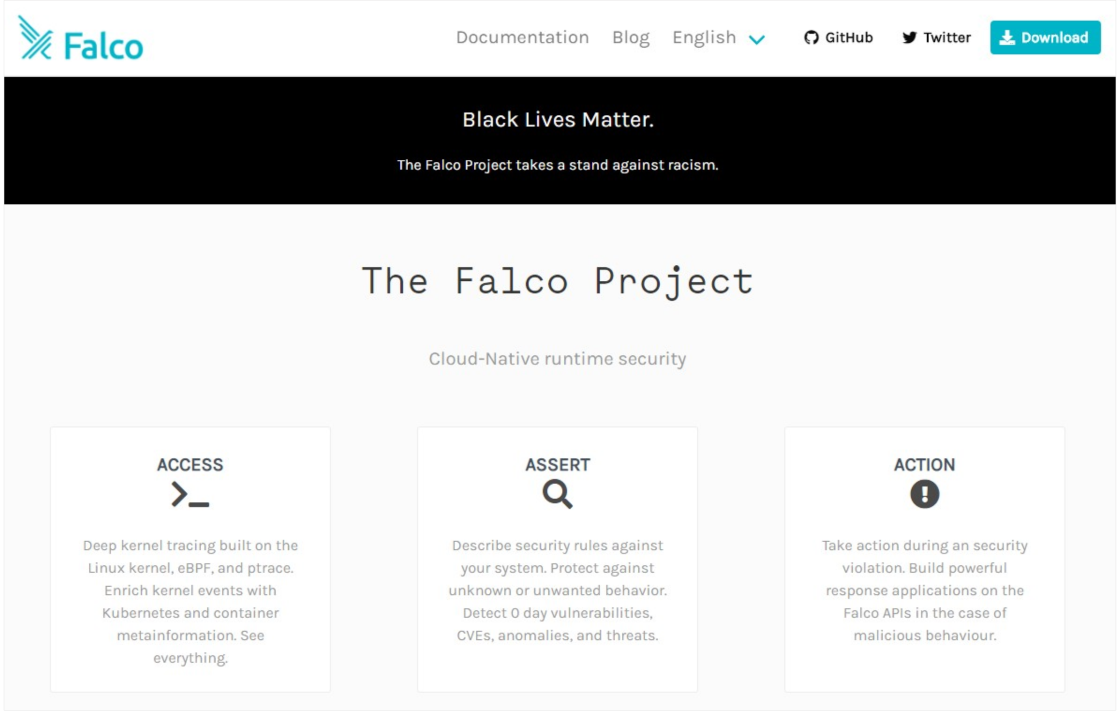
falco.org/docs/

Repositorio git:

github.com/falcosecurity/falco

Blog:

falco.org/blog/



Black Lives Matter.

The Falco Project takes a stand against racism.

The Falco Project

Cloud-Native runtime security

ACCESS

Deep kernel tracing built on the Linux kernel, eBPF, and ptrace. Enrich kernel events with Kubernetes and container metainformation. See everything.

ASSERT

Describe security rules against your system. Protect against unknown or unwanted behavior. Detect 0 day vulnerabilities, CVEs, anomalies, and threats.

ACTION

Take action during an security violation. Build powerful response applications on the Falco APIs in the case of malicious behaviour.