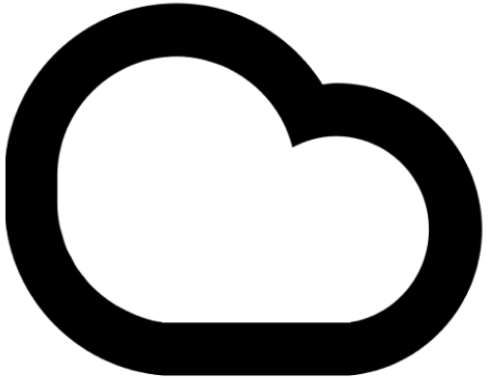


CloudConf

TORINO martedì 11 OTTOBRE **2022**

Osservabilità e **Sicurezza** ai tempi dei container: *vediamoci chiaro* con un approccio **Cloud Native**

by **ANDREA VIVALDI**

Team Leader & Solution Architect @Vista Technology

WE DRIVE YOUR **CLOUD NATIVE** JOURNEY

MI PRESENTO, PIACERE DI CONOSCERVI!

Mi chiamo **ANDREA VIVALDI**

- Sono Team Leader e Solution Architect, in ambito DevOps e tecnologie abilitanti al Cloud Native, per **Vista Technology**
- Sono da sempre appassionato ai temi di **Automazione**, **Osservabilità**, **Telemetria** e **Monitoraggio**
- Ultimamente mi districo tra **Secure DevOps** e **Network Automation**

https://github.com/andreavivaldi

https://www.linkedin.com/in/andreavivaldi/

andrea.vivaldi@vistatech.it

https://www.vistatech.it/

PARTIAMO SUBITO DA UN PRESUPPOSTO

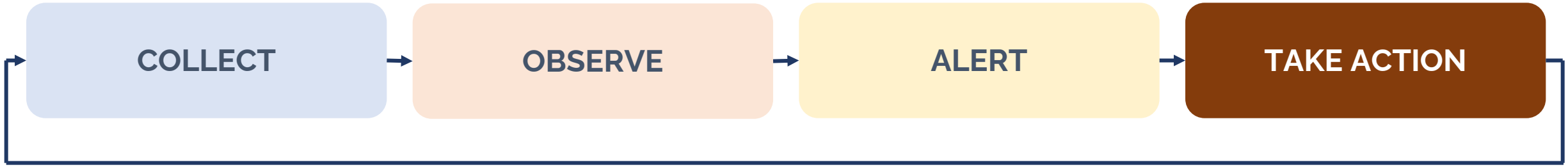
Kubernetes è il «*nuovo*» **Sistema Operativo** nel mondo Cloud

[cit. Loris Degioanni, CTO e Founder Sysdig]

ERA «CLOUD-NATIVE»: NUOVE SFIDE

- Approccio «*all*»**OPS**
  - Qualsiasi cosa, dalle infrastrutture di rete ai server allo sviluppo applicativo, si basa sui principi e sulle pratiche del DevOps
  - Contesto comune tra team eterogenei
- **Hyper-fragmentation**
  - Architetture orientate ai Microservizi
- **Velocità** e **resilienza**
  - Necessità di velocizzare i processi di rilascio e la raccolta dei dati di feedback
- Componenti **effimeri** ed estramente **«dispersivi»**
  - *«non posso misurare ciò che non riesco a vedere»*
- **Osservabilità** come mattone fondamentale su cui costruire tutti i nostri castelli (e quindi anche la **Sicurezza**)

MODELLO CLOSED-LOOP



CONTINUOUS FEEDBACK	Integrare continuous monitoring & observability nei propri processi di CI/CD, per ottenere feedback in real-time
PERFORMANCE	Ottenere la maggior parte di dati, out-of-the-box, nel minor tempo possibile. Estrarli e visualizzarli in maniera agile
COVERAGE	Garantire il pieno accesso la copertura a tutti i team coinvolti
AUTOMATION	Avere dati che siano utili per le toolchain, in maniera tale che possano reagire ad eventi e triggerare automazioni

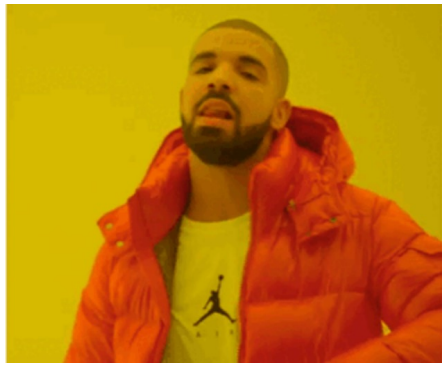
MA HO GIÀ TANTI TOOL A DISPOSIZIONE...

STRUMENTI LEGACY

- Non «container-native»
- Non tengono in considerazione il contesto K8S
- Nessun concetto di DevOps

SOLUZIONI IPER-SPECIFICHE

- Instrumentazione spesso invasiva
- Limitato il contesto K8S
- Mancanze in termini di scalabilità e granularità del dato



STRUMENTI PURPOSE-BUILT

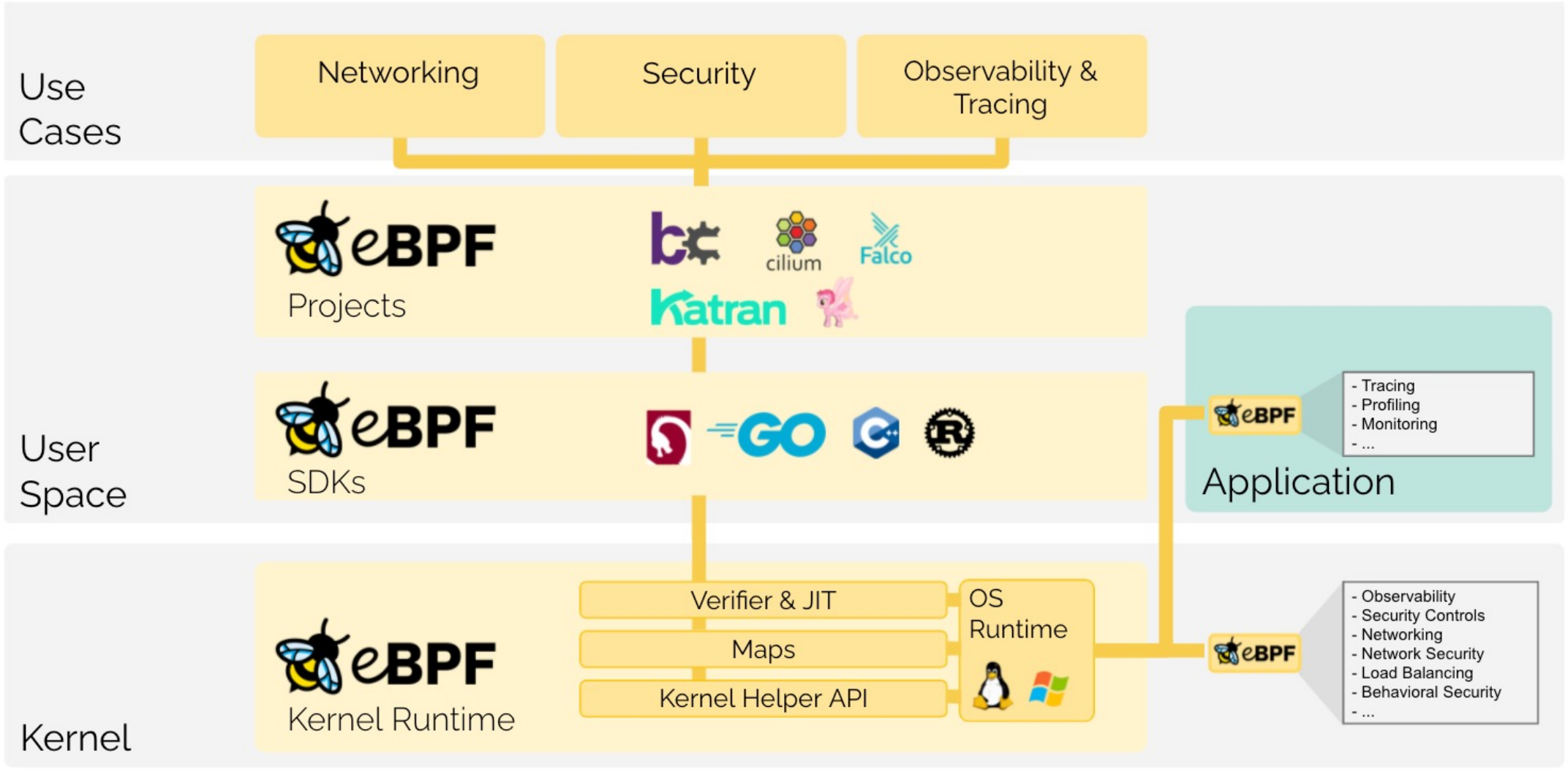
Tecnologie nate e/o pensate per un mondo Cloud Native


SO...
WHAT DOES THIS ALL MEAN?
makeameme.org

UNA POSSIBILE STRADA TECNOLOGICA: **eBPF**

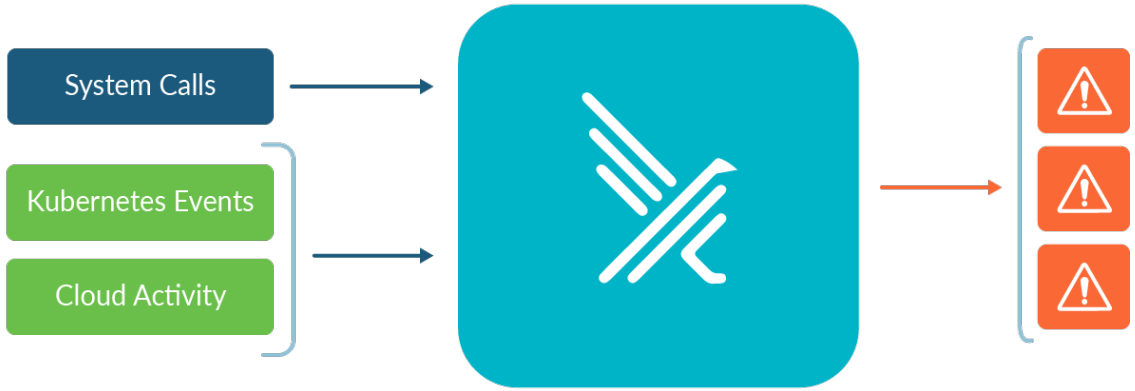
- *Extended Berkeley Paket Filter*
- Tecnologia **kernel** che consente ai programmi di girare come se fossero dentro una **sandbox**, in cui poter beneficiare di **capabilities** specifiche del kernel senza aggiungere moduli o toccare il codice sorgente
- I programmi eBPF sono **event-driven** e vanno in esecuzione nel momento in cui il kernel o un'applicazione passa attraverso un certo **hook**
- Esistono **hooks predefiniti**
  - system calls
  - function entry/exit
  - kernel tracepoints
  - network events
  - … e tanti altri …

UNA POSSIBILE STRADA TECNOLOGICA: **eBPF**



DALLA TECNOLOGIA AL PRODOTTO

FALCO



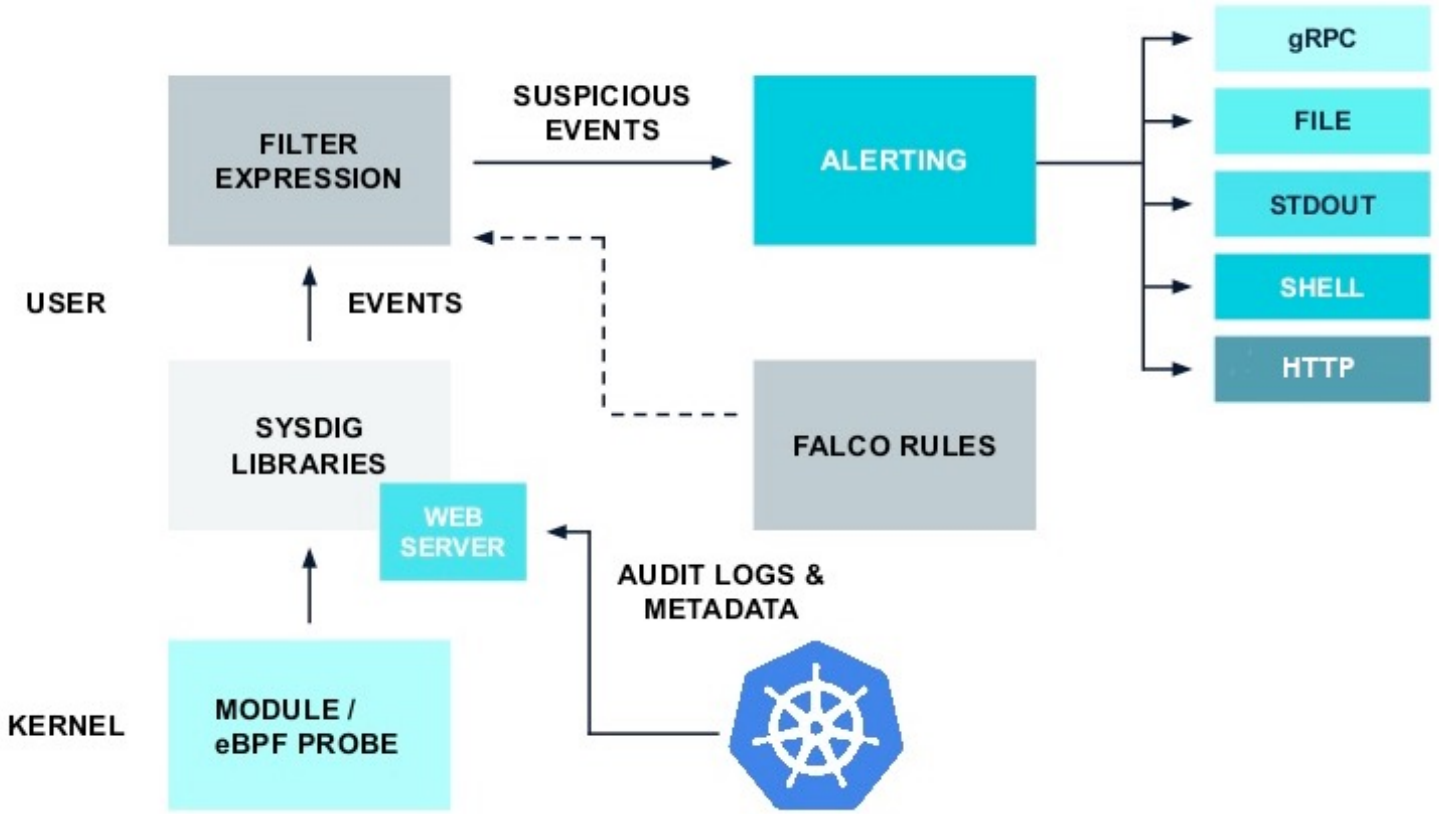
- **Open Source**
- Creato da **Sysdig** nel **2016**
- Primissimo progetto di runtime security ad essere «*incubato*» dentro la **CNCF**

- Cloud Native **runtime Security** & **Visibility**
- Motore di **Threat Detection**, standard *de-facto* in ambito K8S
- Utilizza la tecnologia **eBPF** per intercettare
  - System calls
  - Eventi kernel
  - Kubernetes audit events
  - Eventi Cloud
- **Monitoraggio** del comportamento di un cluster sotto tutti i punti di vista
  - Accesso a dati sensibili
  - Attività dei nodi del cluster
  - Attività dei POD

COME FUNZIONA

Falco utilizza i dati raccolti dai driver kernel per:

- Parsare le system call a livello Kernel
- Verificare i dati in base al motore di Rules
- Allertare in output in caso di violazione



COSA CERCA DI PRECISO FALCO?

- Una shell aperta all'interno di un container/POD in Kubernetes
- Un container che gira in privileged mode, o che monta un path sensibile direttamente dall'host (es: /proc)
- Un processo server che «spawna» un processo figlio inaspettatamente
- Lettura inaspettate di file particolare, come ad esempio /etc/shadow
- Un file non-device scritto sotto /dev
- Un binario standard di sistema, come ad esempio ls, che esegue una connessione verso l'esterno
- …

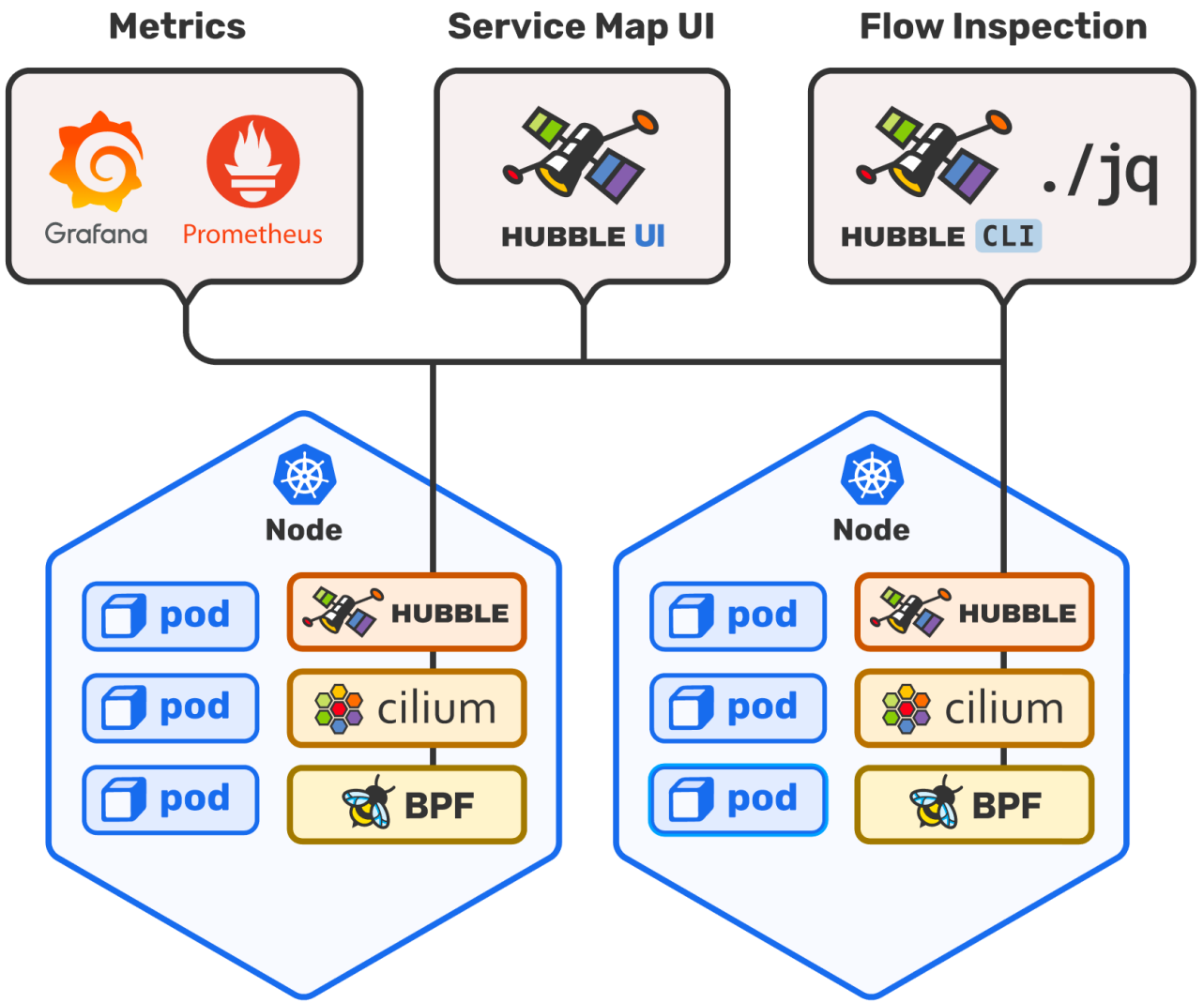
(l'elenco non è ovviamente esaustivo…)

DALLA TECNOLOGIA AL PRODOTTO

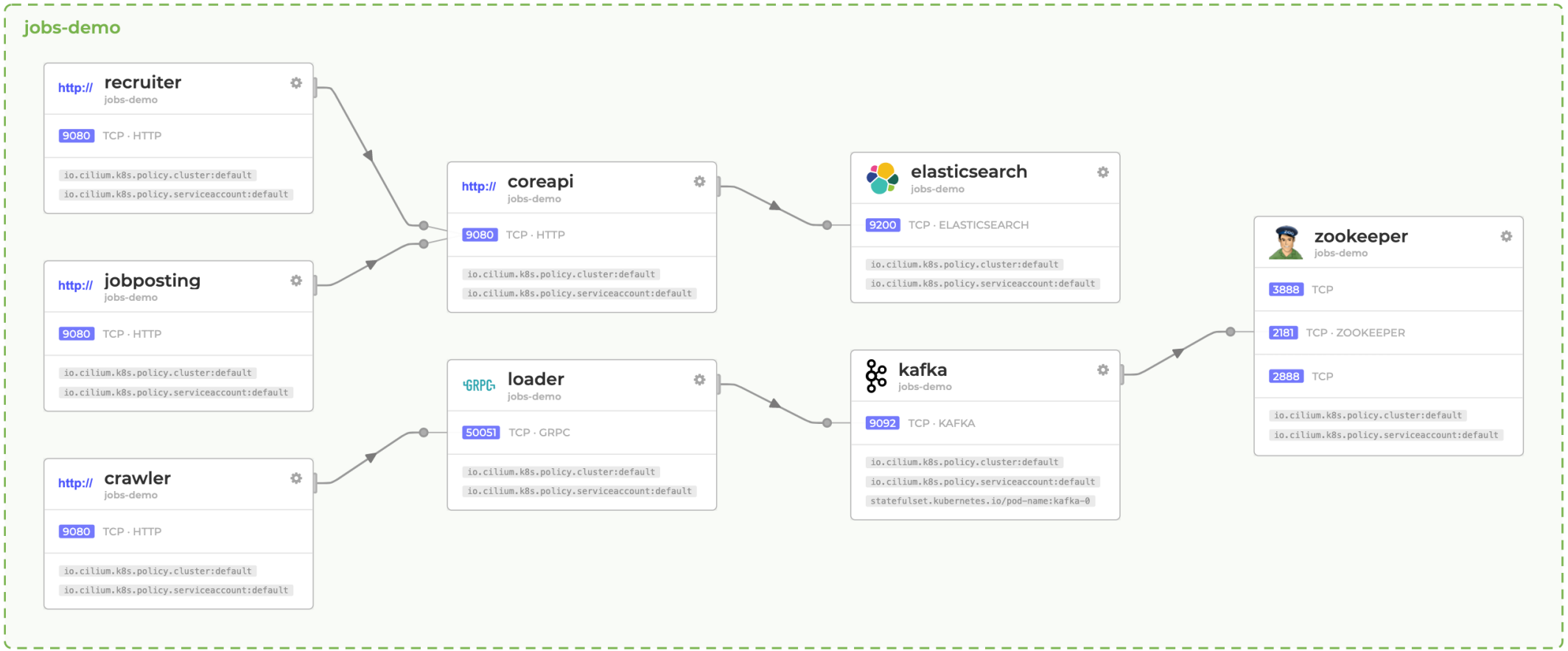
CILIUM + HUBBLE

- Cilium è un progetto open, una **CNI** per **Kubernetes**, basata sulla tencologia eBPF, nativamente pensata per feature come **sicurezza osservabilità** e **performance** in ambito workload Cloud Native
- Hubble si basa su Cilium per fornire un tool di visibilità, tracciabilità ed osservabilità
  - Risponde alle classiche domande:
    - Quale microservizio comunica con chi? Si può avere una topologia?
    - Quali chiamate vengono effettuate e cosa contengono?
    - È colpa del DNS o del trasporto?
    - La comunicazione è rotta a livello 4 o a livello 7?
    - Ci sono delle comunicazioni bloccate per colpa di una network policy?
    - …
- Integrazione con strumenti per raccolta metriche e log aggregation

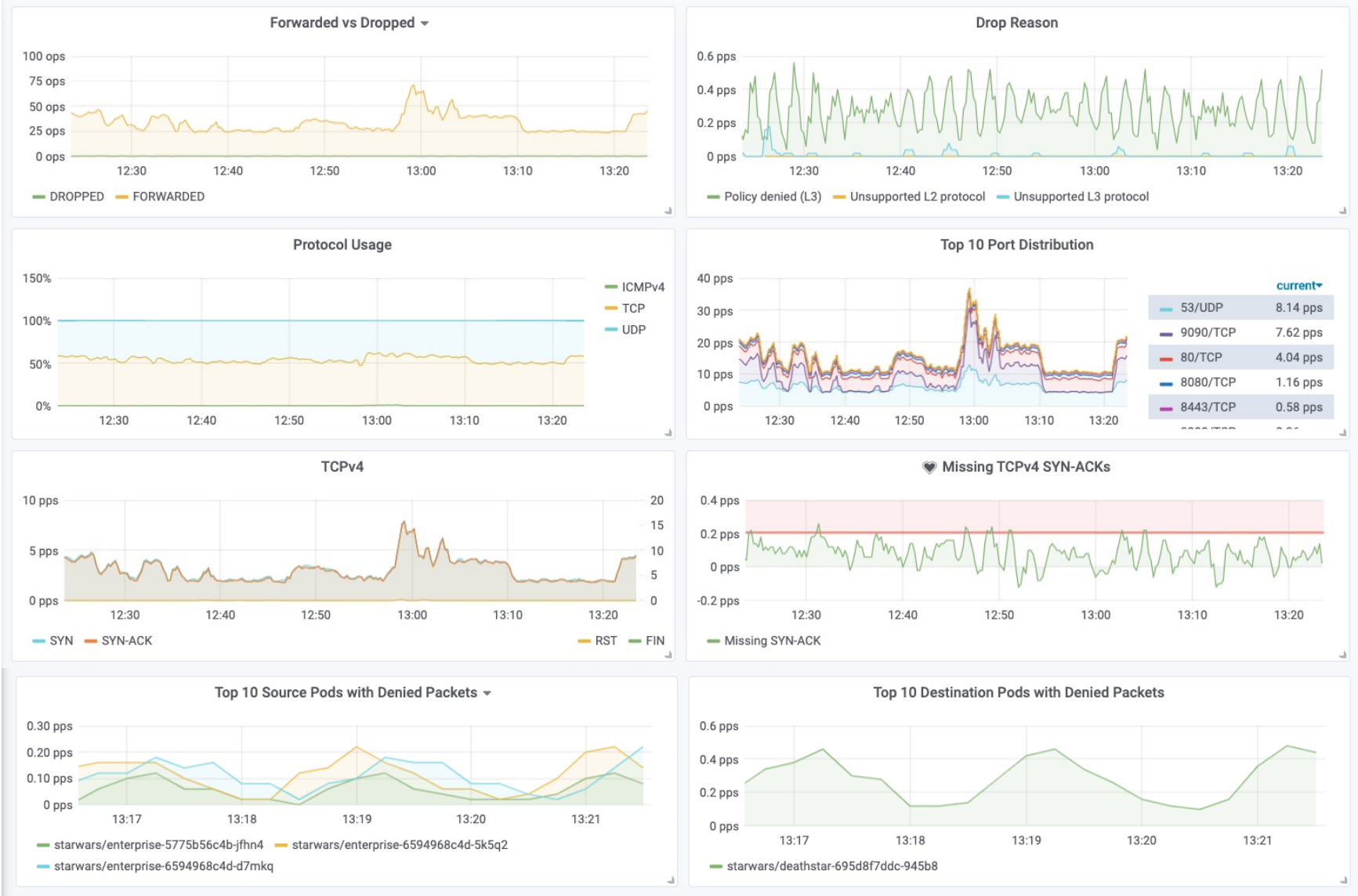
COME FUNZIONANO



HUBBLE TOPOLOGY MAP



CILIUM & HUBBLE METRICS

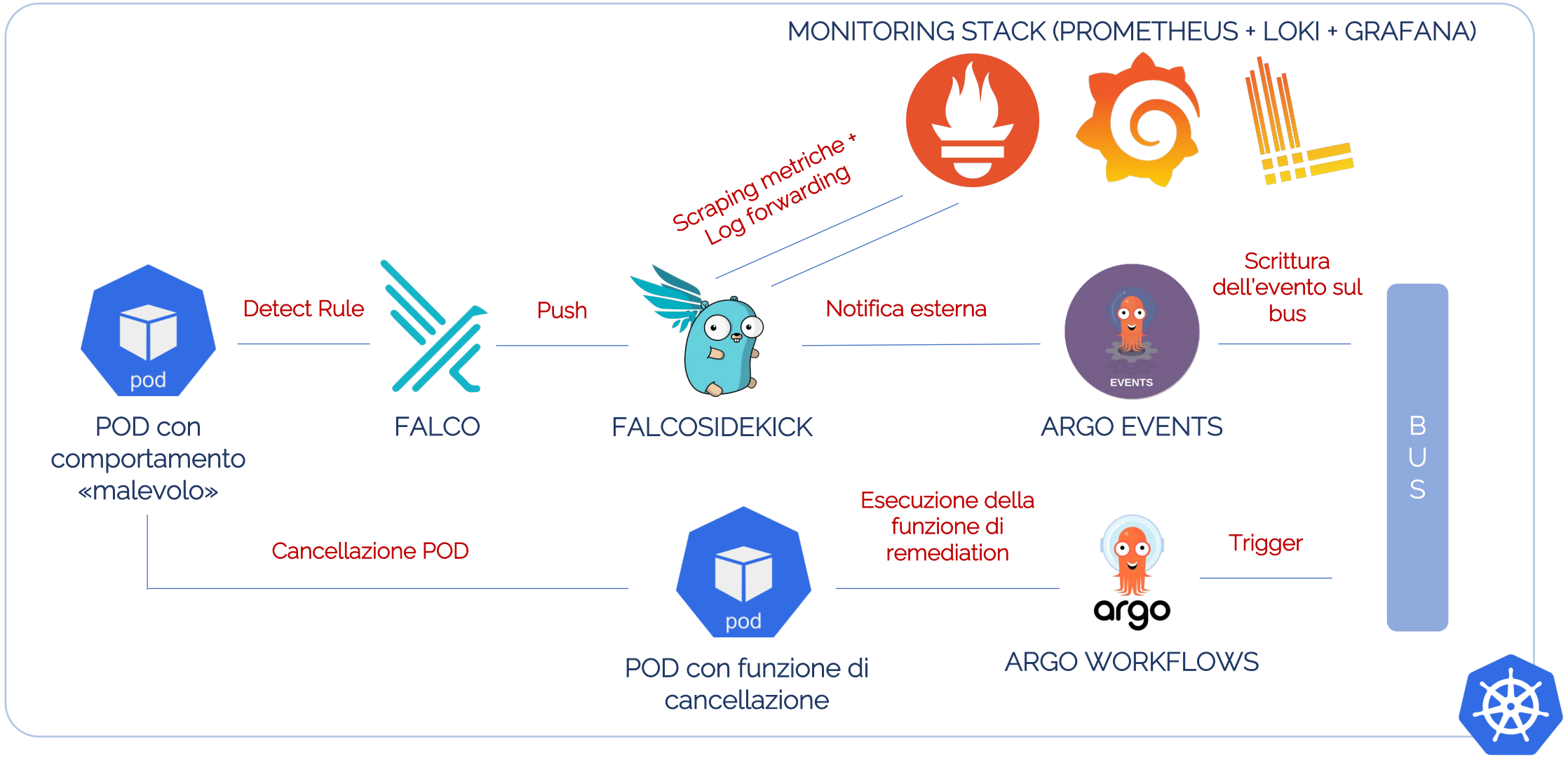


ORA FACCIAMO UN ESERCIZIO…

Consideriamo il seguente caso d'uso:

- POD di prova deployato su un cluster k8s per testare comportamenti «malevoli»
  - Detect di una connessione network verso un URL specifico tramite una rule Falco
  - Detect dell'esecuzione di una shell all'interno di un container
- A seguito del detect agire in maniera automatizzata, con un sistema di gestione di azioni ed eventi, per «killare» il POD in questione
- Integrare il tutto con un sistema di metriche e log collection (Prometheus+Grafana+Loki)

IL RISULTATO FINALE



DEMO TIME

… che sarà registrata, perché mi sono dimenticato di omaggiare i «demo gods», quindi non posso rischiare …

CREDITS

- https://sysdig.com/blog/ (immagini e articoli)
- https://falco.org/docs (immagini e articoli)
- https://github.com/falcosecurity/falco
- https://github.com/falcosecurity/falcosidekick
- https://ebpf.io/what-is-ebpf/ (immagini e articoli)
- https://falco.org/blog/falco-on-rke-with-rancher/ (demo)
- https://github.com/falcosecurity/charts/tree/master/falco
- https://falco.org/blog/intro-k8s-security-monitoring/
- https://falco.org/blog/falco-kind-prometheus-grafana/ (demo)
- https://falco.org/blog/extend-falco-outputs-with-falcosidekick/ (demo)
- https://falco.org/blog/falcosidekick-response-engine-part-5-argo/ (demo)
- https://cilium.io/ (immagini e definizioni)
- https://github.com/cilium/hubble/ (immagini e definizioni)
- https://sysdig.com/blog/unexpected-domain-connection/

GRAZIE A TUTTI PER L'ATTENZIONE!

DOMANDE….?