ISOVALENT

eBPF for Security

Liz Rice | @lizrice

Chief Open Source Officer, Isovalent | CNCF Governing Board | OpenUK Board

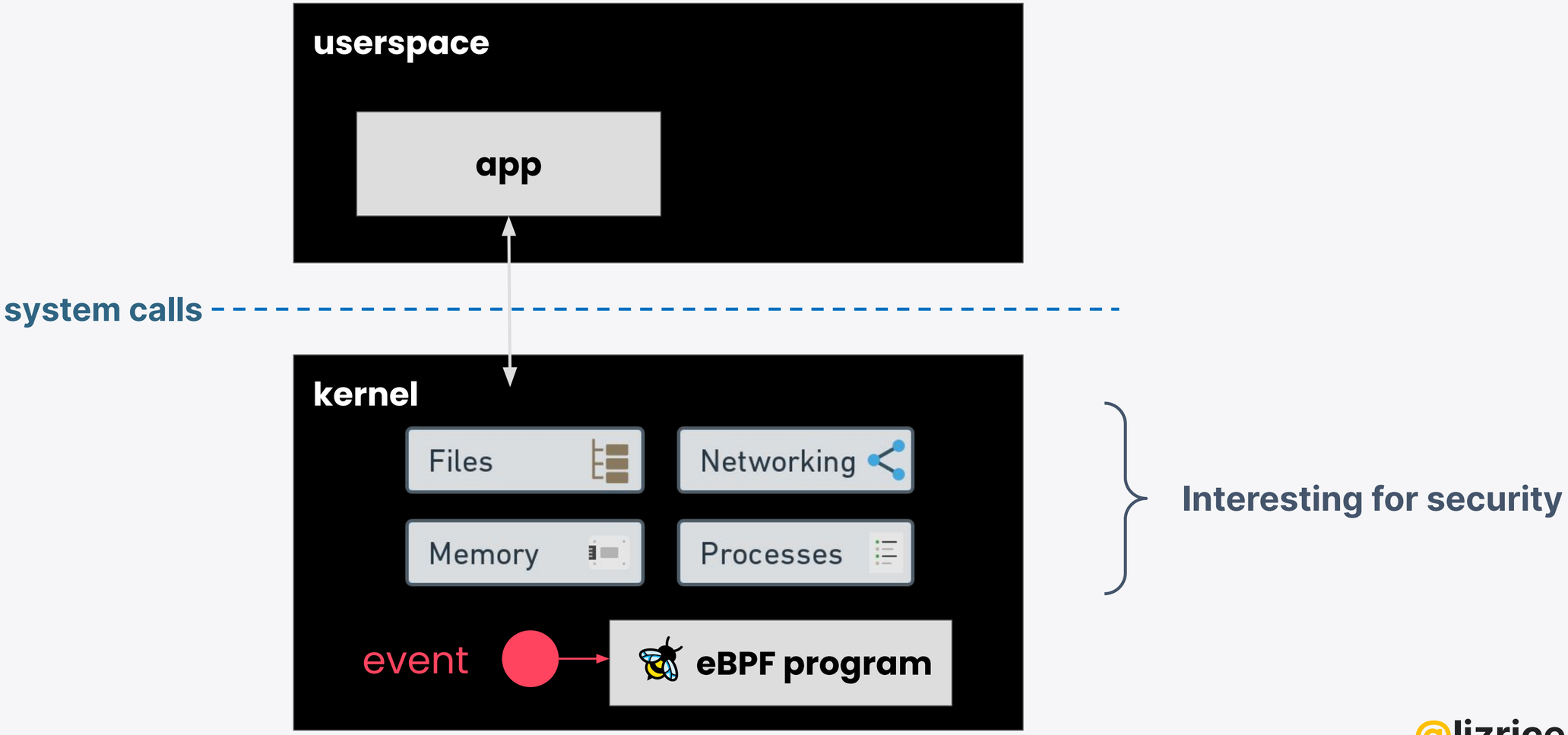
ISOVALENT

What is  eBPF ?

Makes the kernel programmable

ISOVALENT

Run custom code in the kernel



@lizrice

ISOVALENT

eBPF Hello World

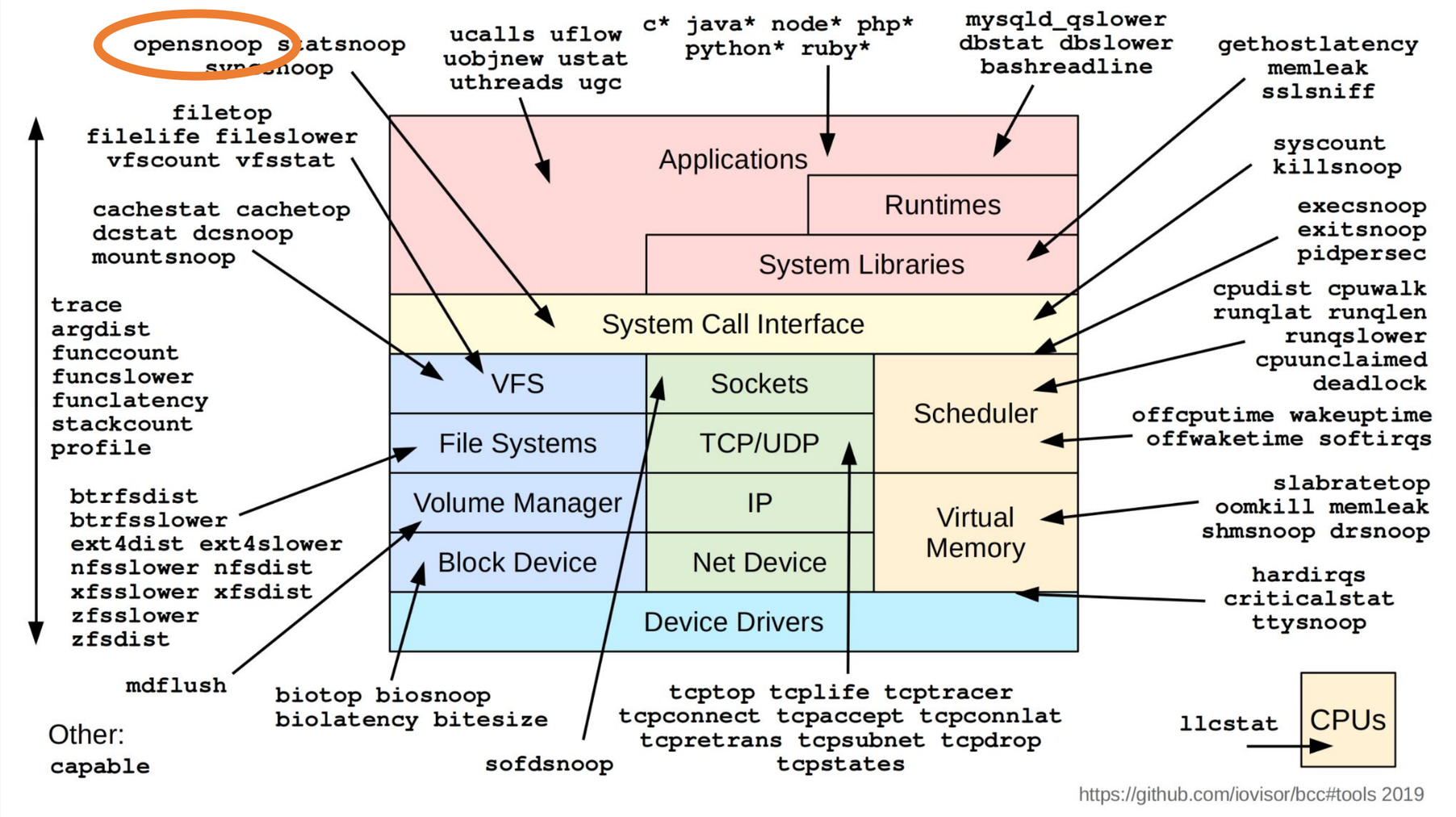
```
SEC("kprobe/sys_execve")
int hello(void *ctx)
{
    bpf_trace_printk("Hello World!");
    return 0;
}
```

\+ userspace code to load eBPF program

Info about process that called execve syscall

```
$ sudo ./hello
   bash-20241   [004] d...  84210.752785: 0: Hello World!
   bash-20242   [004] d...  84216.321993: 0: Hello World!
   bash-20243   [004] d...  84225.858880: 0: Hello World!
```

eBPF tracing tools from iovisor/bcc



https://github.com/iovisor/bcc#tools 2019

ISOVALENT

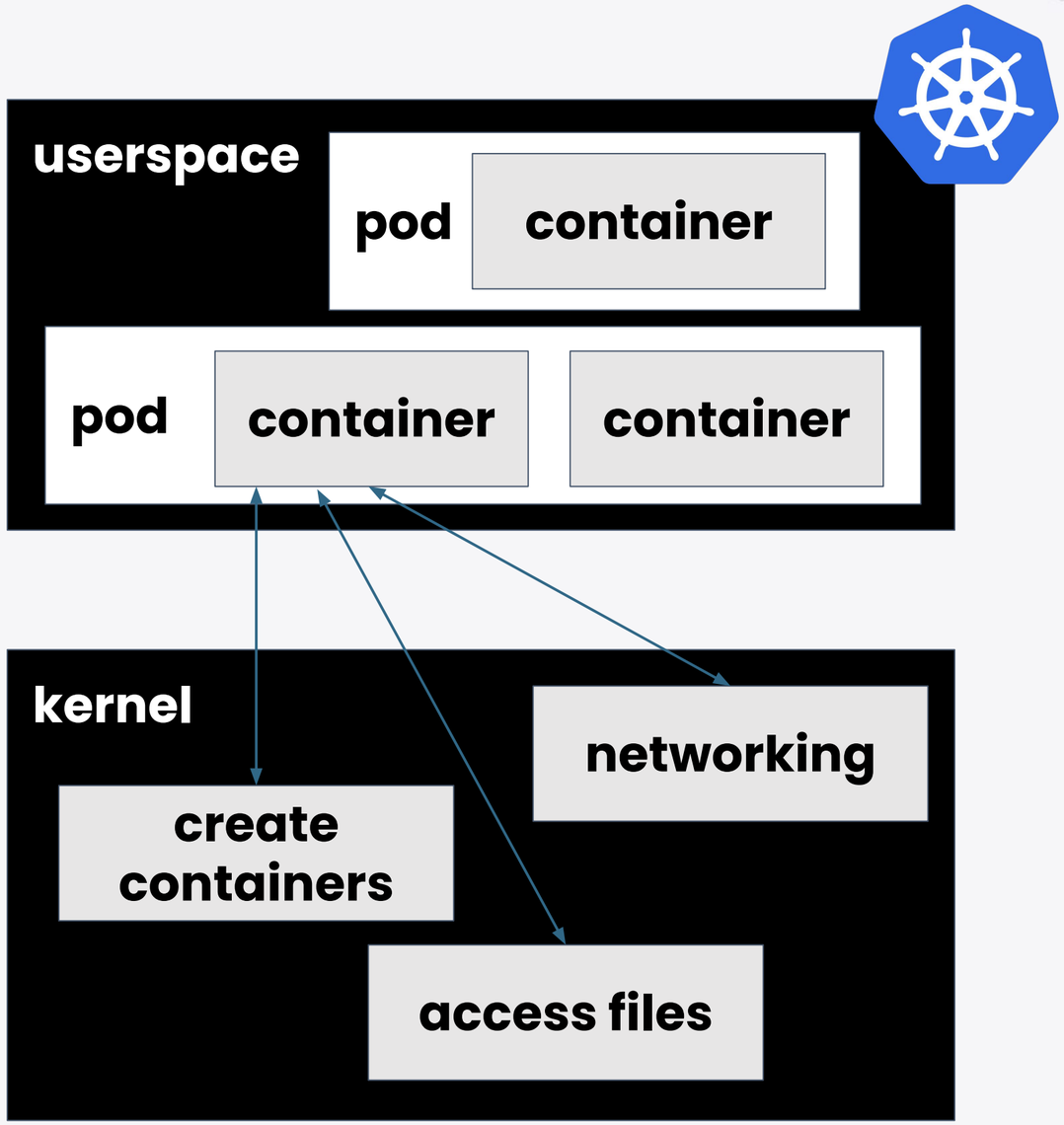
eBPF tracing - opensnoop

```
~/bcc/libbpf-tools$ sudo ./opensnoop
PID    COMM               FD ERR PATH
5040   node               21   0 /proc/5132/cmdline
5040   node               21   0 /proc/6460/cmdline
5040   node               21   0 /proc/6460/cmdline
6461   opensnoop          18   0 /etc/localtime
5040   node               21   0 /proc/5132/cmdline
5040   node               21   0 /proc/6460/cmdline
5060   node               23   0 /home/liz/.vscode-server/data/User/workspaceStorage/48b53
5040   node               21   0 /proc/5132/cmdline
5040   node               21   0 /proc/6460/cmdline
5040   node               21   0 /proc/5132/cmdline
5040   node               21   0 /proc/6460/cmdline
…
```

ISOVALENT

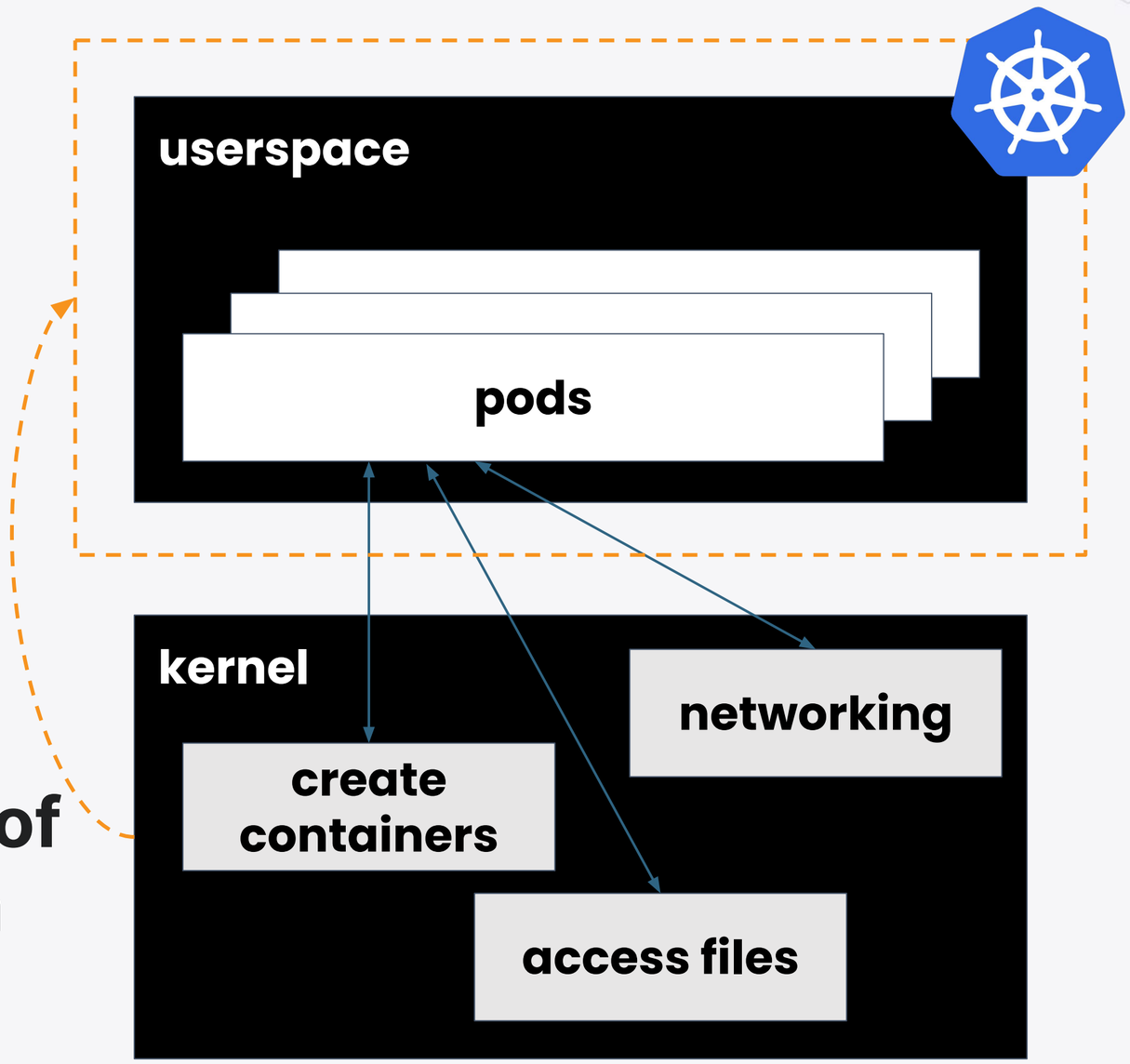
eBPF and Kubernetes

ISOVALENT



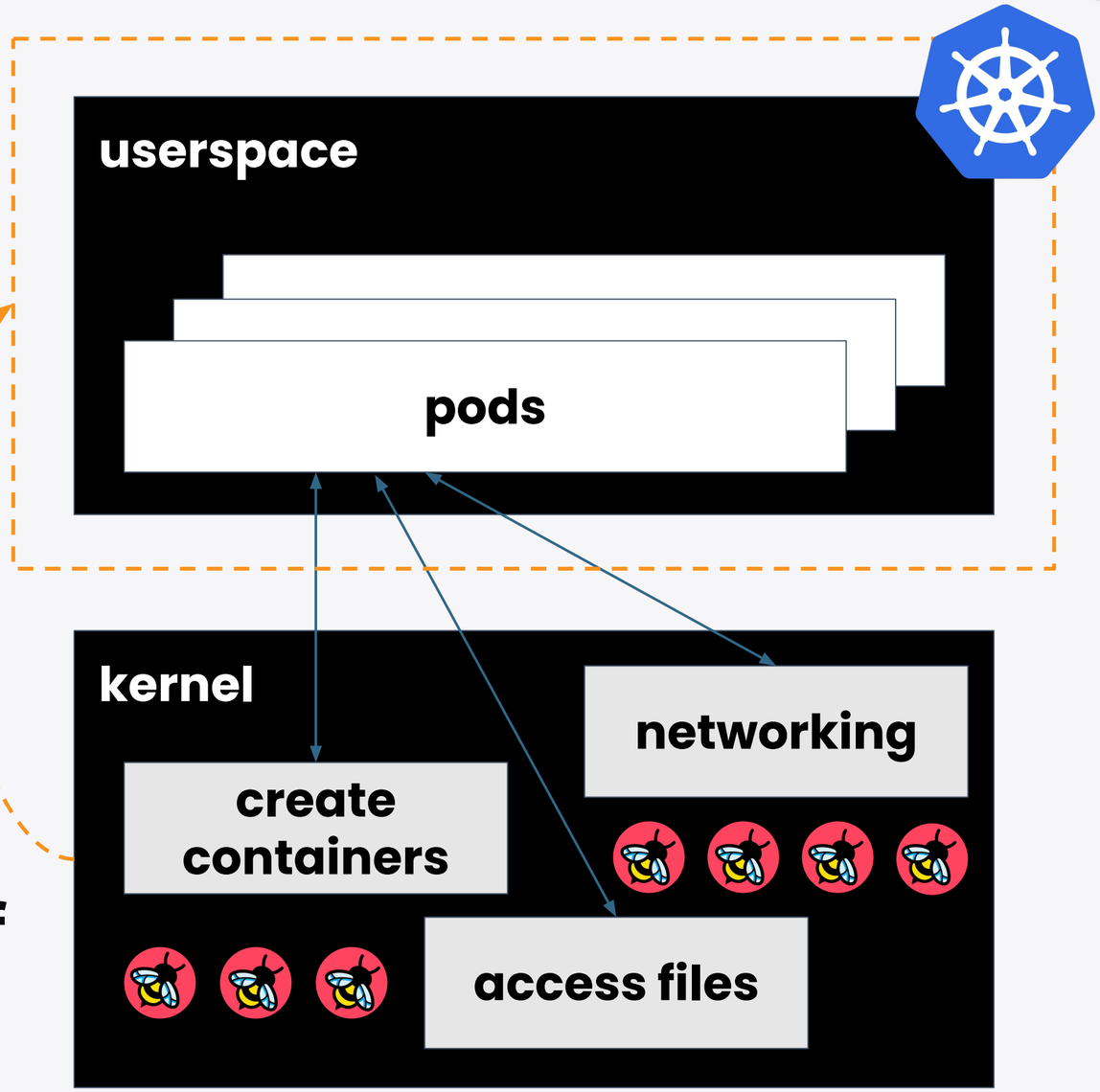
One kernel per host

ISOVALENT



Kernel aware of everything on the host

ISOVALENT



No changes to apps or config needed

eBPF programs can be aware of everything

ISOVALENT

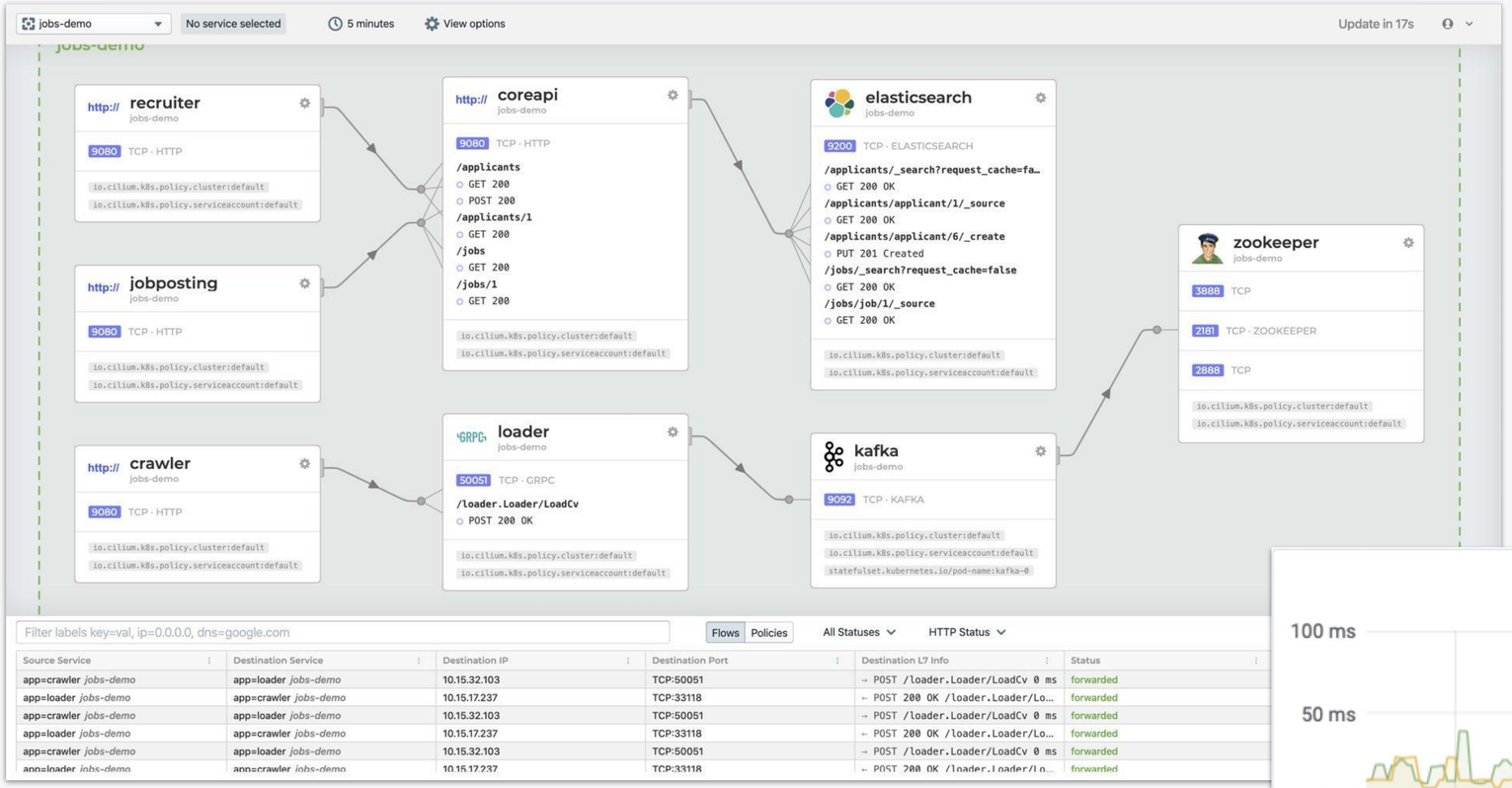
eBPF tracing on Kubernetes - Inspektor Gadget

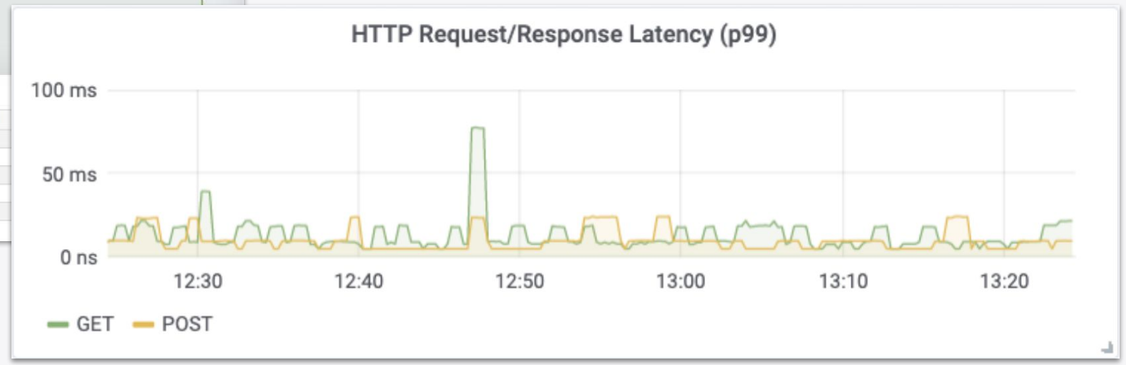
```
$ kubectl gadget trace open
NODE                   NAMESPACE     POD      CONTAINER    PID     COMM    FD  ERR PATH
kind-2-control-plane   default       xwing    spaceship    361876 vi      3     0 /etc/passwd
```

Kubernetes info

ISOVALENT

eBPF observability tools - Cilium Hubble





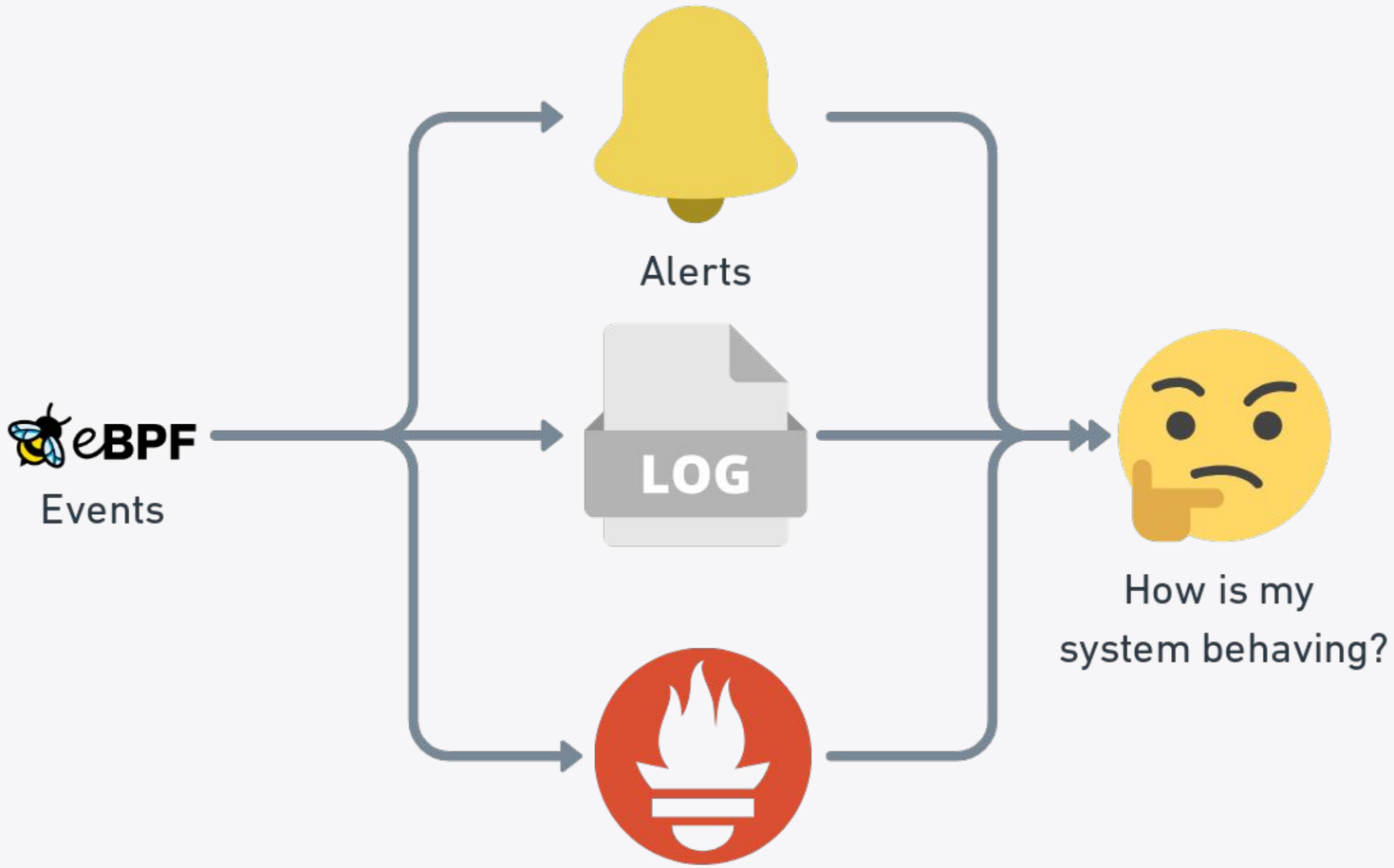
@lizrice

ISOVALENT

eBPF security observability

ISOVALENT

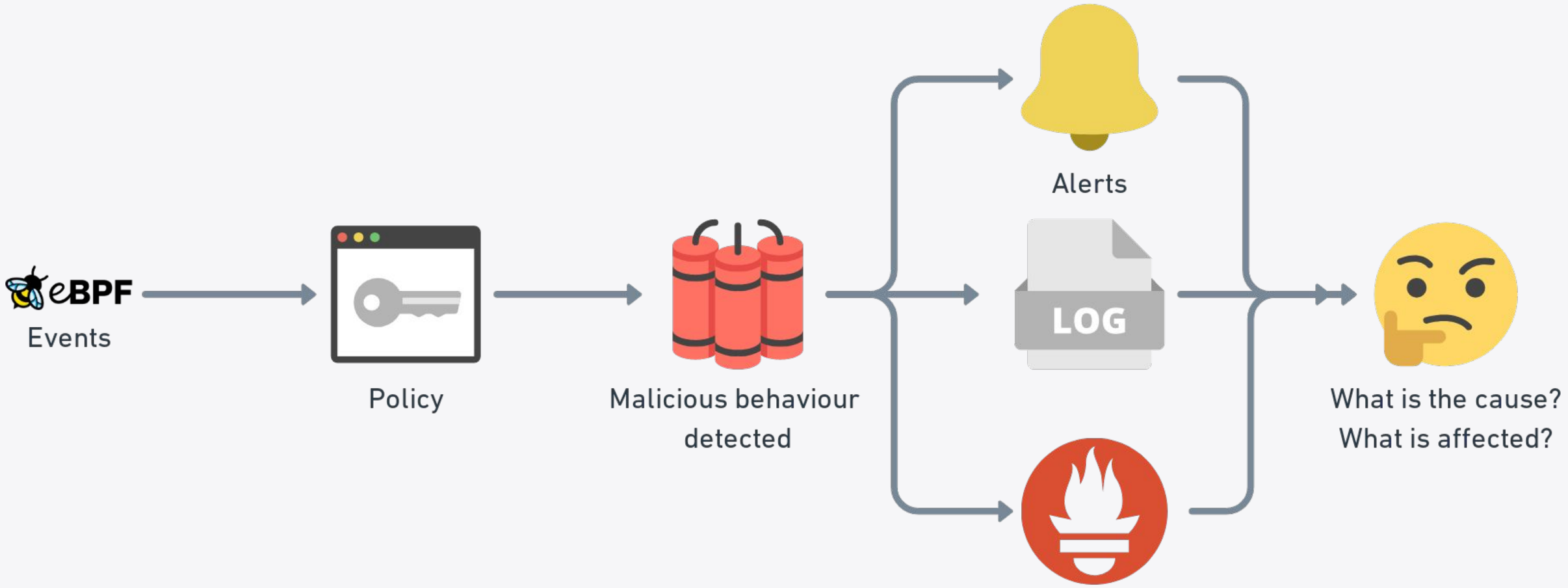
Observability



@lizrice

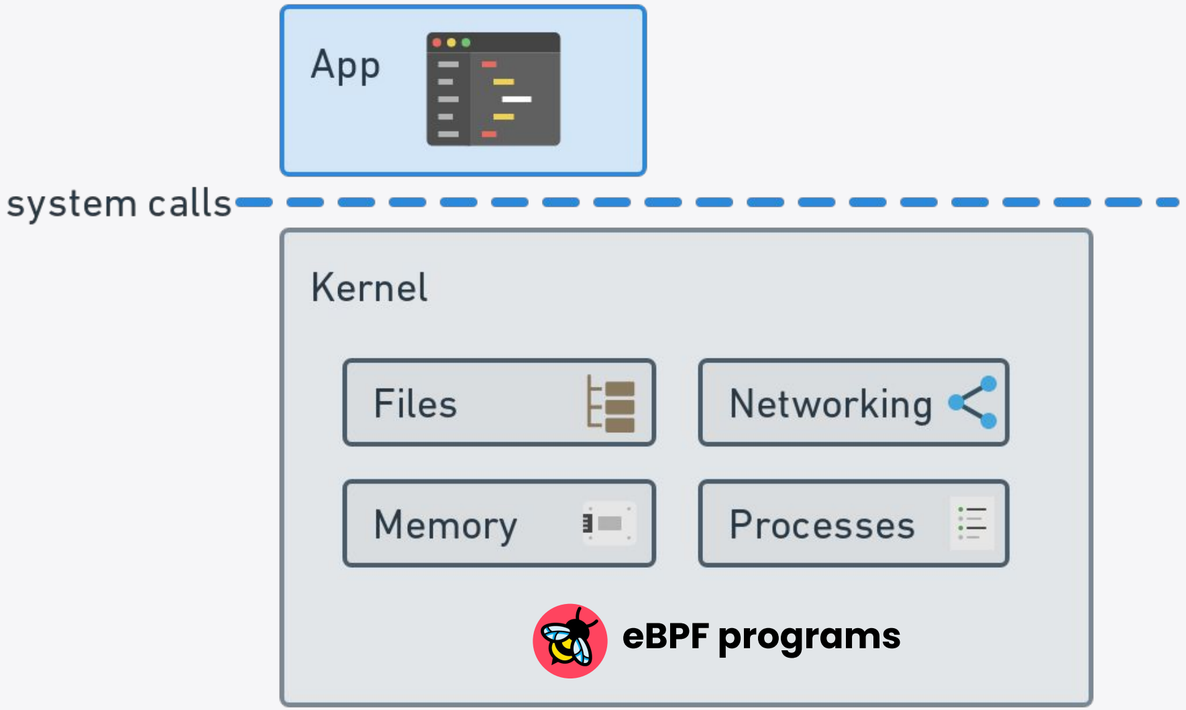
ISOVALENT

Security observability



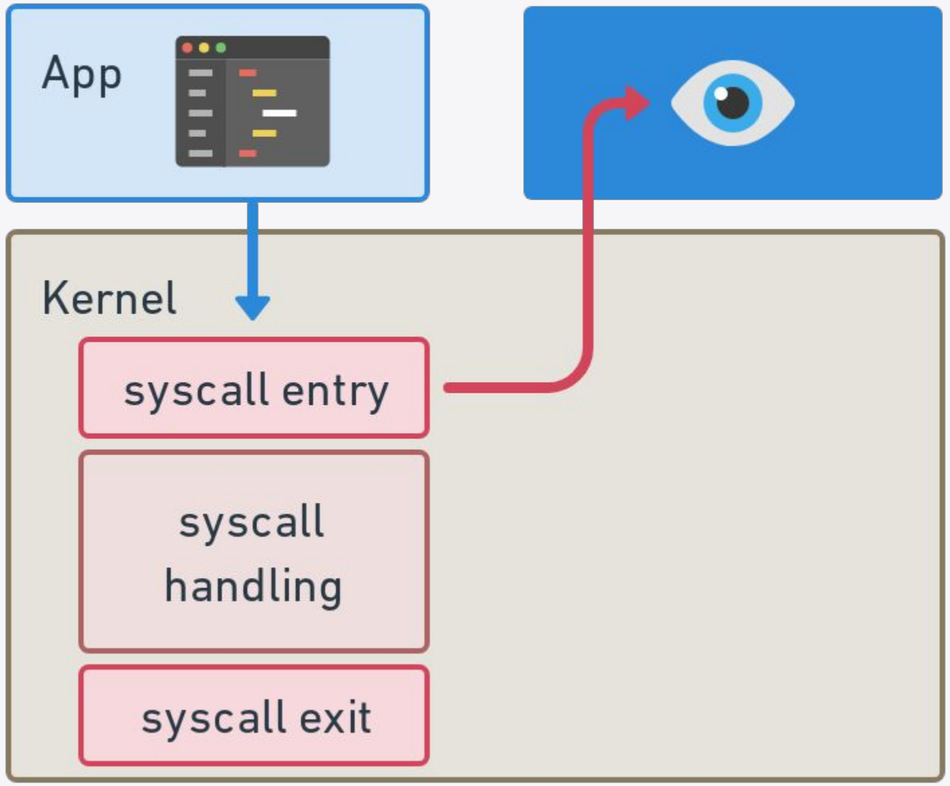
@lizrice

What activity do we care about for security?



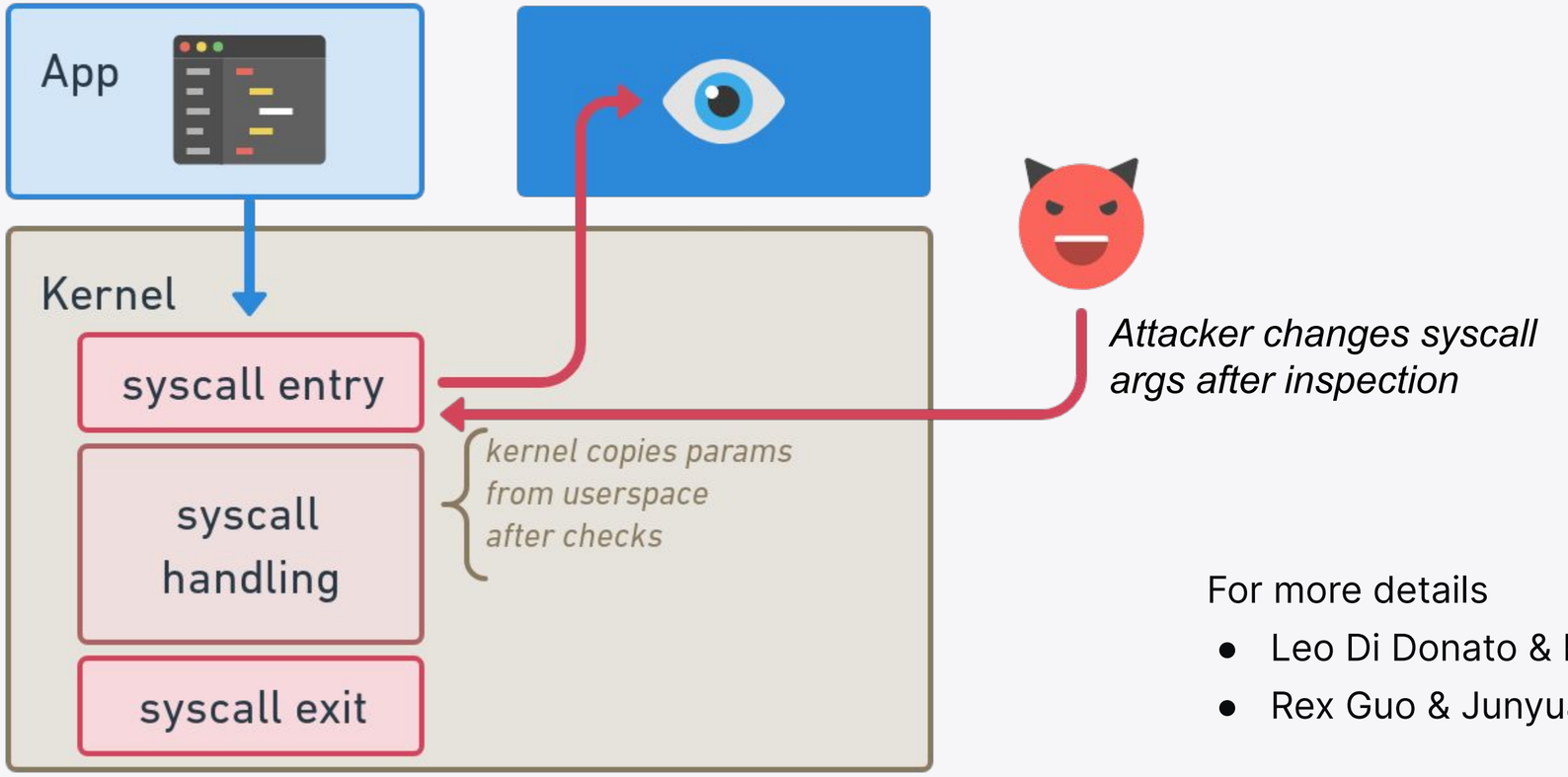
ISOVALENT

Syscall checks within the kernel



ISOVALENT

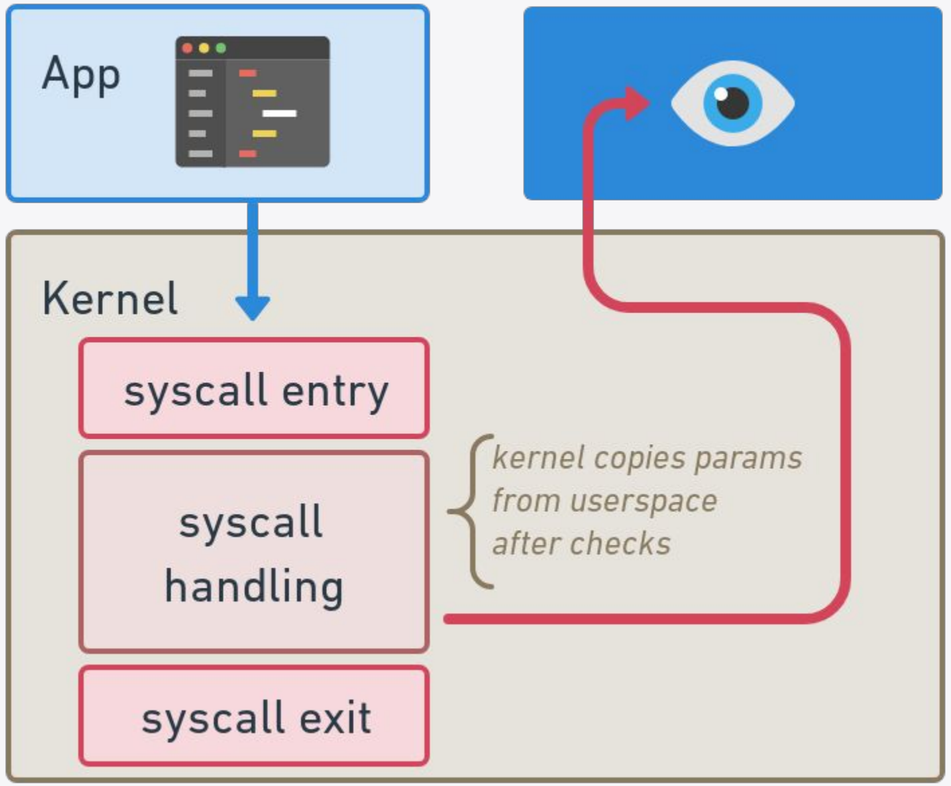
TOCTTOU vulnerabilities with syscalls



For more details

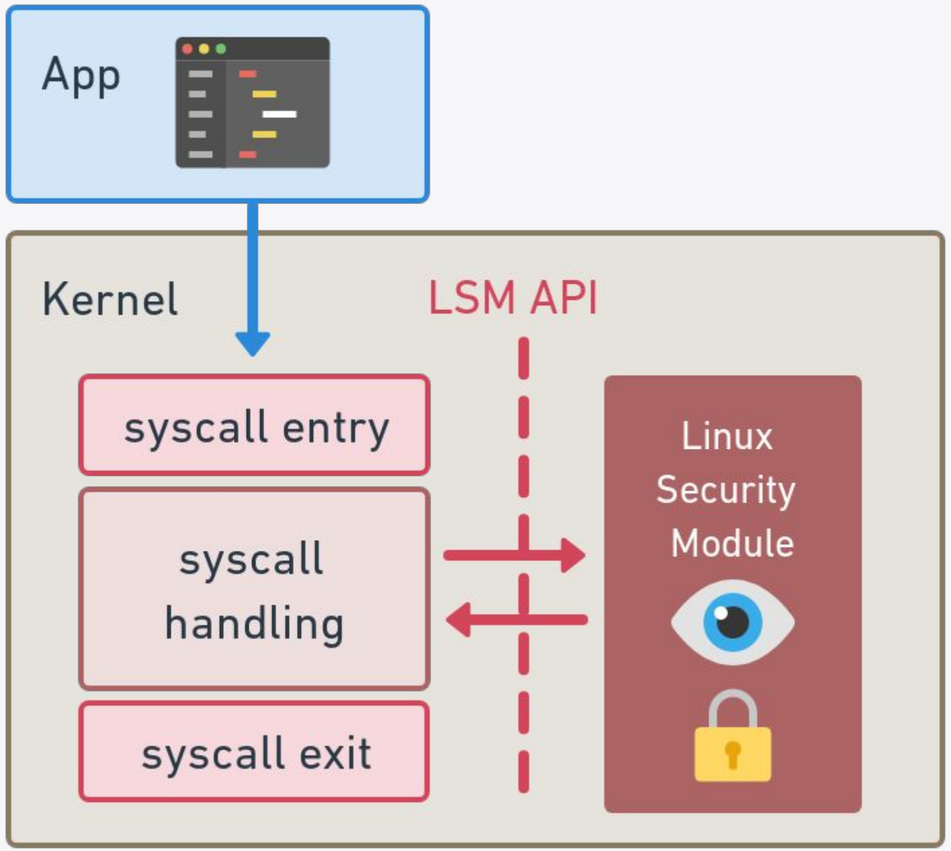
- Leo Di Donato & KP Singh at CN eBPF Day 2021
- Rex Guo & Junyuan Zeng at DEFCON 29 on Phantom attacks

Need to make the check at the right place



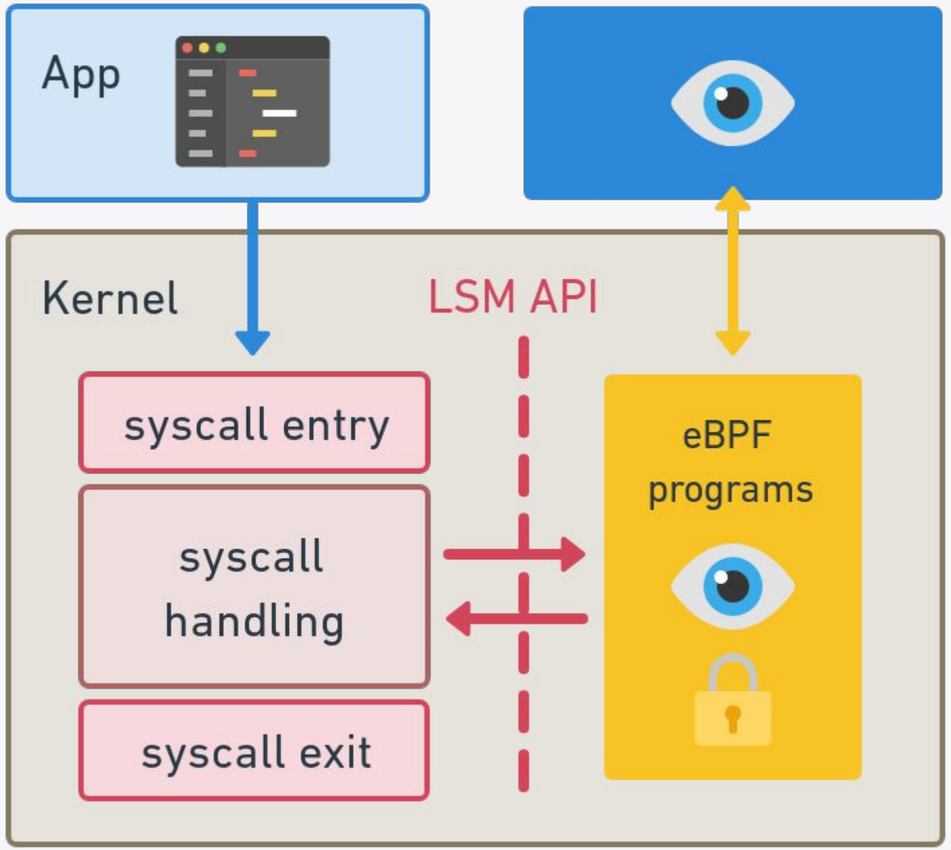
ISOVALENT

Linux Security Modules



- Stable interface
- Safe places to make checks

BPF LSM



- Stable interface
- Safe places to make checks

+ **eBPF benefits**
- Dynamic
- Protect pre-existing processes

ISOVALENT

BPF LSM hook has kernel info populated

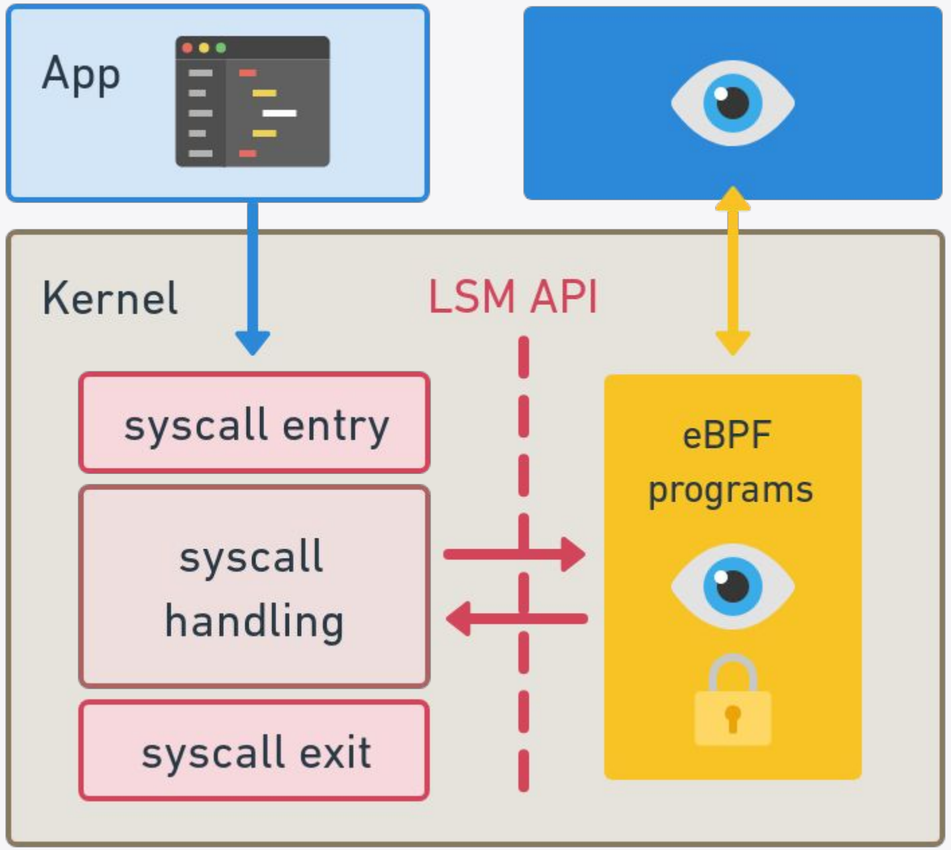
```
SEC("lsm/path_chmod")
int BPF_PROG(path_chmod, const struct path *path, umode_t mode)
{
    bpf_printk("lsm path_chmod %s\n", path->dentry->d_iname);
    return 0;
}
```

```
$ sudo ./chmoddemo &
[1] 7631
$ sudo cat /sys/kernel/debug/tracing/trace_pipe
           chmod-7776    [001] d... 38197.342160: bpf_trace_printk: lsm path_chmod liz
```

Filename known to kernel

ISOVALENT

BPF LSM



- Stable interface
- Safe places to make checks

\+ **eBPF benefits**

- Dynamic
- Protect pre-existing processes

But needs **kernel 5.7+**

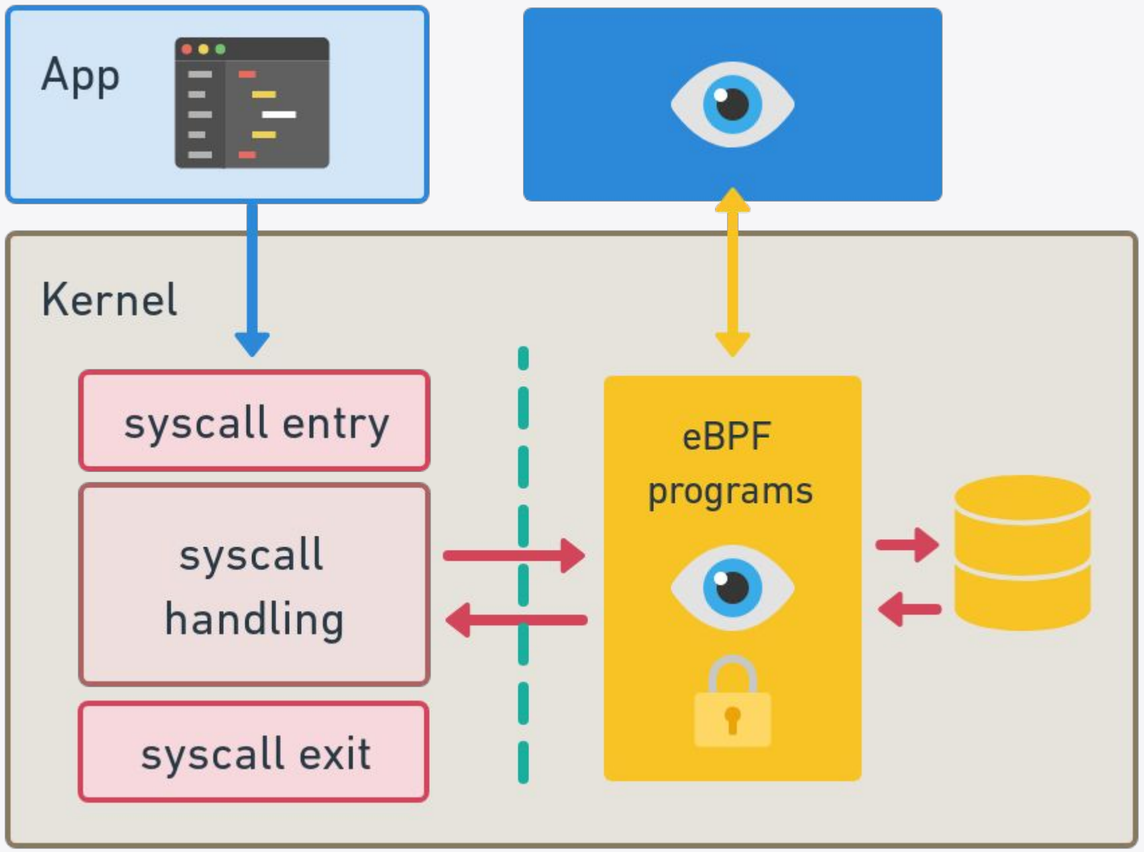
& Kubernetes context?

ISOVALENT

How stable is the Linux kernel?

ISOVALENT

Cilium Tetragon



- Safe places to make checks

+ **eBPF benefits**
- Dynamic
- Protect pre-existing processes

Uses **kernel knowledge** to hook into sufficiently stable functions

Adds Kubernetes context

@lizrice

A Tetragonisca angustula bee guarding the nest-entrance

Photo credit: Bibafu

ISOVALENT

Cilium Tetragon tracing policy

```
apiVersion: cilium.io/v1alpha1
kind: TracingPolicy
metadata:
 name: "etc-files"
spec:
 kprobes:
 - call: "fd_install"
…
      matchArgs:
      - index: 1
        operator: "Prefix"
        values:
        - "/etc/"
…
```

+ Policy “follows” file descriptor through read, write & close events

ISOVALENT

Cilium Tetragon observe security events

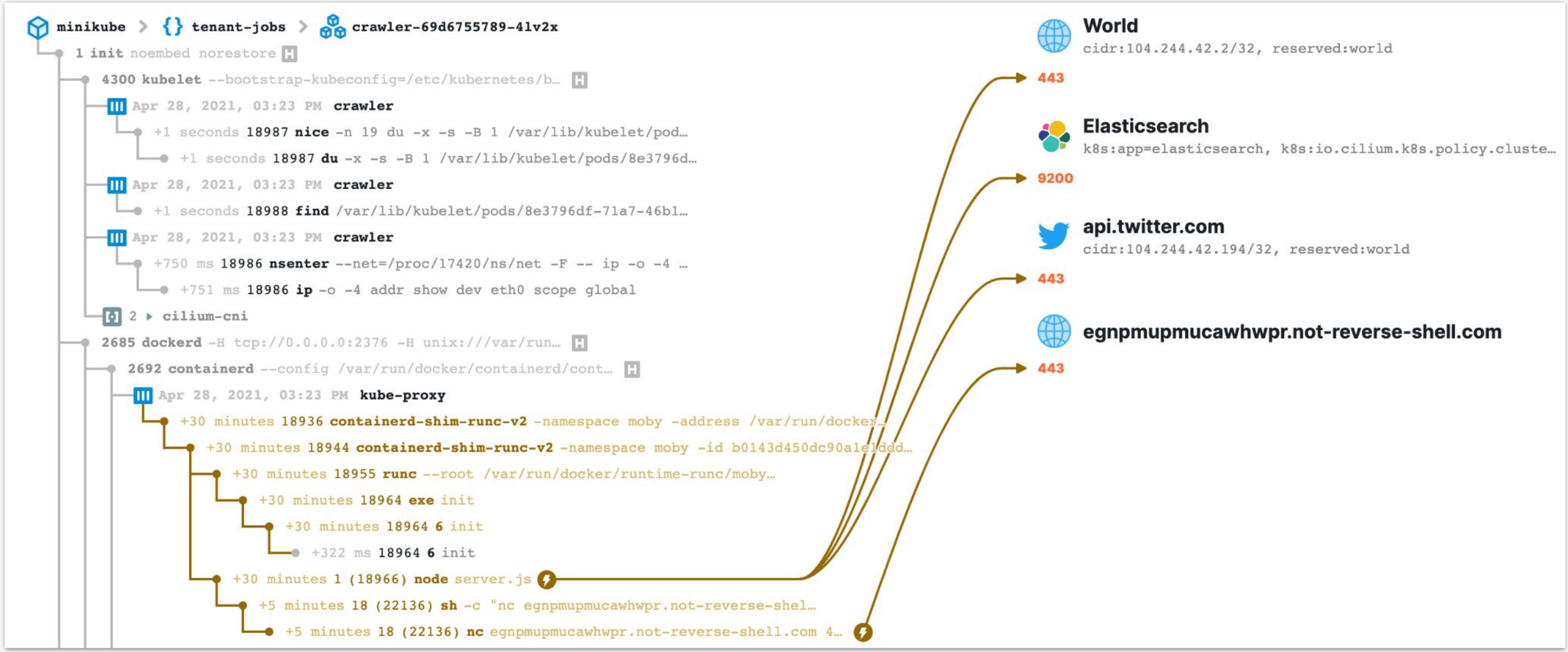
```
$ kubectl logs ds/tetragon -c export-stdout -f | tetra getevents -o compact
🚀 process default/xwing /usr/bin/vi /etc/passwd
📬 open    default/xwing /usr/bin/vi /etc/passwd
📪 close   default/xwing /usr/bin/vi
📬 open    default/xwing /usr/bin/vi /etc/passwd
📝 write   default/xwing /usr/bin/vi /etc/passwd 1275 bytes
📪 close   default/xwing /usr/bin/vi
💥 exit    default/xwing /usr/bin/vi /etc/passwd 0
```

Kubernetes info

Policy events

ISOVALENT

Combined network and runtime visibility



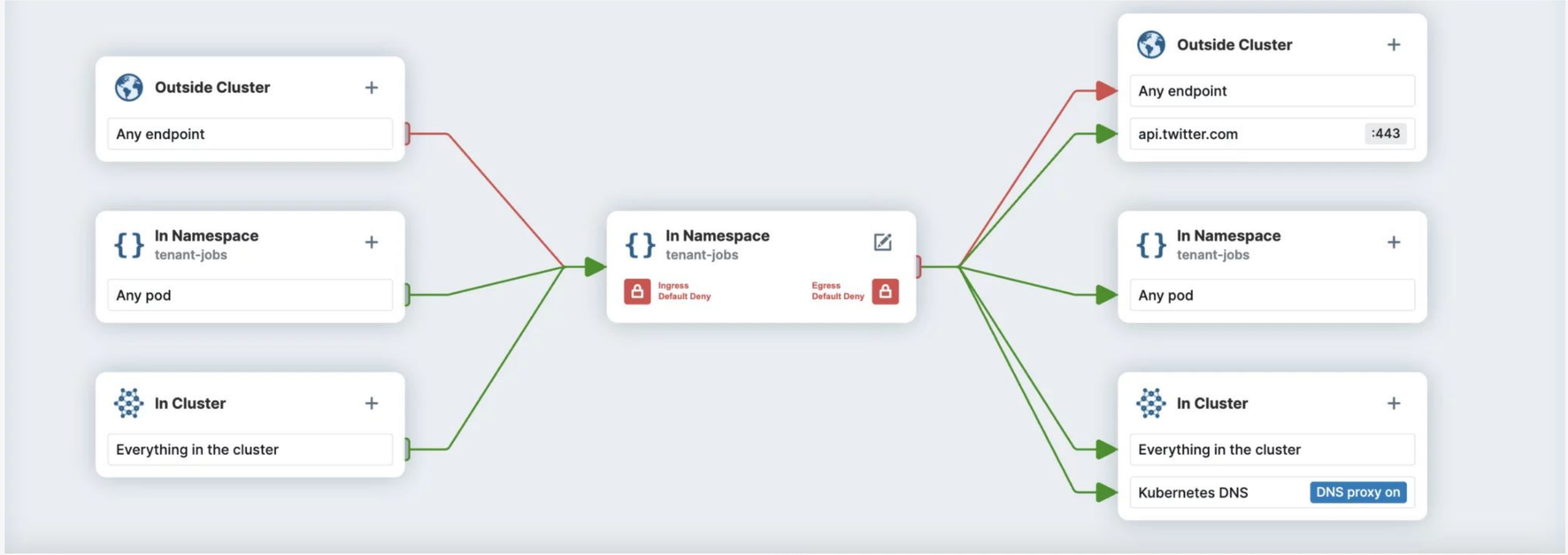
@lizrice

ISOVALENT

eBPF preventative runtime security

ISOVALENT

Cilium network policy → eBPF programs drop packets



Kubernetes | Cilium | Download

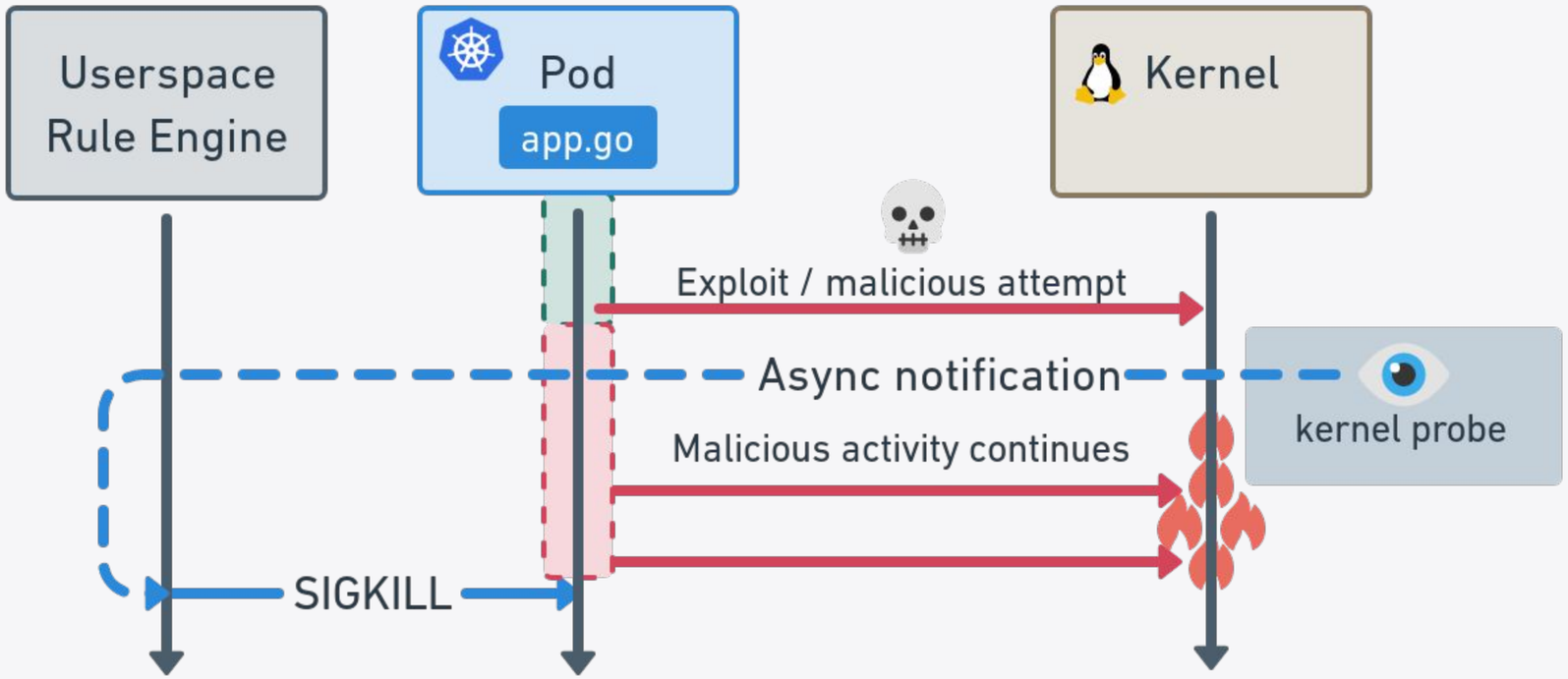
```
21        - ports:
22            - port: "53"
23              protocol: ANY
24          rules:
25            dns:
26              - matchPattern: "*"
27    - toFQDNs:
28        - matchName: api.twitter.com
29      toPorts:
30        - ports:
31            - port: "443"
```

Source Identity	Destination Identity	Verdict
crawler *tenant-jobs*	api.twitter.com	forwarded
crawler *tenant-jobs*	elasticsearch *tenant-jobs*	forwarded
crawler *tenant-jobs*	elasticsearch *tenant-jobs*	forwarded
crawler *tenant-jobs*	api.twitter.com	forwarded
loader *tenant-jobs*	kafka *tenant-jobs*	forwarded
coreapi *tenant-jobs*	elasticsearch *tenant-jobs*	forwarded
jobposting *tenant-jobs*	coreapi *tenant-jobs*	forwarded
jobposting *tenant-jobs*	coreapi *tenant-jobs*	forwarded
coreapi *tenant-jobs*	elasticsearch *tenant-jobs*	forwarded
kafka *tenant-jobs*	zookeeper *tenant-jobs*	forwarded
coreapi *tenant-jobs*	elasticsearch *tenant-jobs*	forwarded
recruiter *tenant-jobs*	coreapi *tenant-jobs*	forwarded
recruiter *tenant-jobs*	coreapi *tenant-jobs*	forwarded
loader *tenant-jobs*	kafka *tenant-jobs*	forwarded

@lizrice

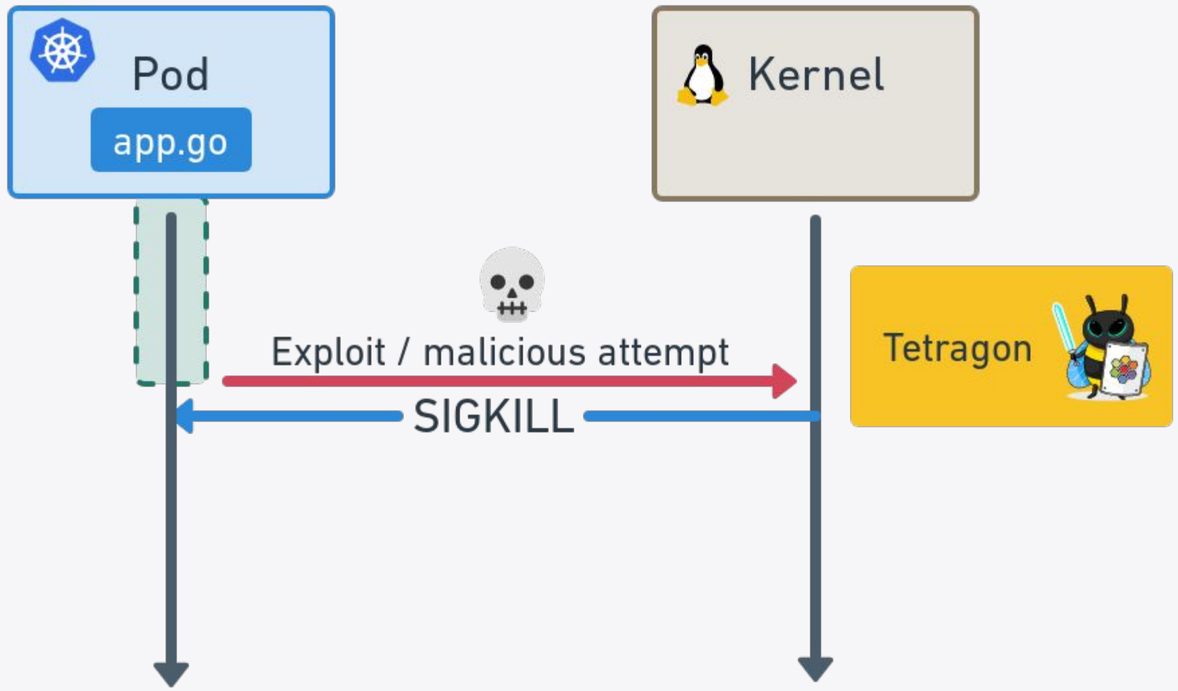
ISOVALENT

Preventative actions from user space



ISOVALENT

Preventative actions from kernel



@lizrice

ISOVALENT

Cilium Tetragon observe

```
$ kubectl logs ds/tetragon -c export-stdout -f | tetra getevents -o compact
🚀 process default/xwing /usr/bin/vi /etc/passwd
📬 open    default/xwing /usr/bin/vi /etc/passwd
📪 close   default/xwing /usr/bin/vi
📬 open    default/xwing /usr/bin/vi /etc/passwd
📝 write   default/xwing /usr/bin/vi /etc/passwd 1269 bytes
💥 exit    default/xwing /usr/bin/vi /etc/passwd SIGKILL
```

Killed before write

ISOVALENT

eBPF security

- Dynamic instrumentation
- Zero app modifications
- Contextual information, Kubernetes identity-aware

ISOVALENT

Isovalent Security Summer School 2023!

Summer is here! And it is a great time to relax, enjoy the sun, recharge - and learn something new! Team Isovalent invites you to our virtual Security Summer School where you can level up your skills with hands-on labs. Learn how Cilium, Tetragon, and Hubble help improve Kubernetes security.

Earn a swag box by completing all 3 sessions!

@lizrice

ISOVALENT

ebpf.io/summit-2023

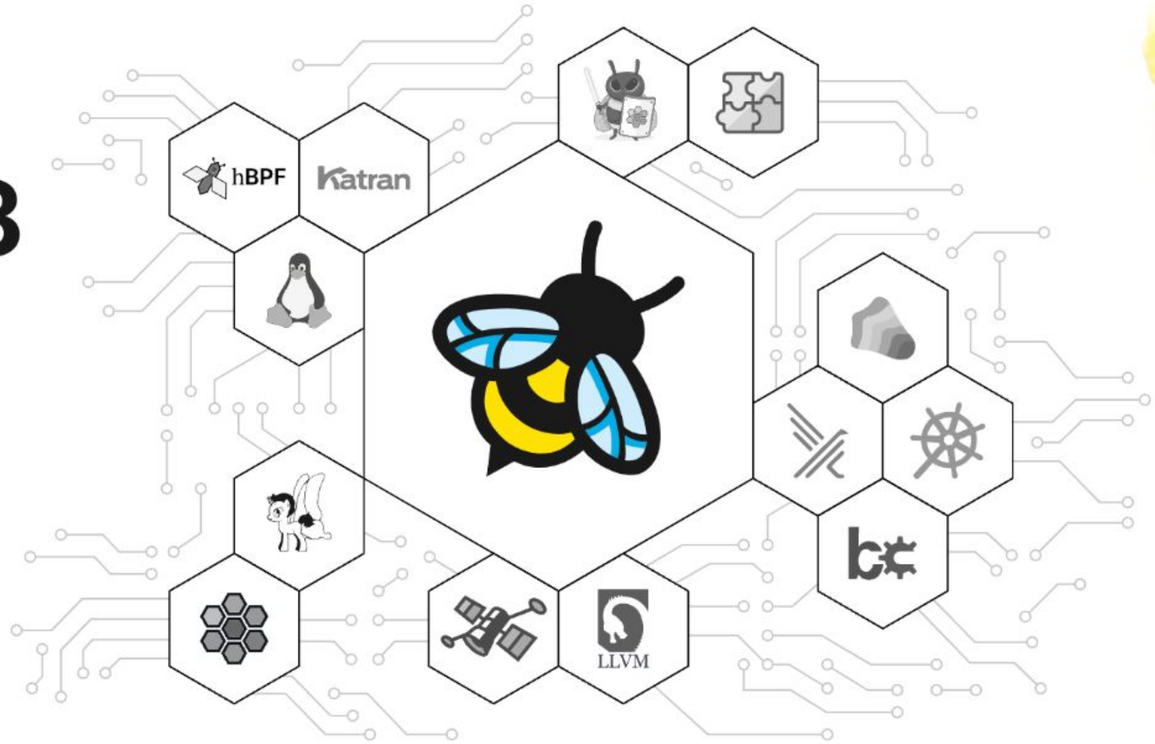
SEPTEMBER 13, 2023

eBPF Summit 2023

Welcome to the eBPF Summit, a virtual event for all things within the Open Source eBPF ecosystem. This event for the eBPF community is aimed at new and existing members wishing to learn and grow and includes hands-on technologists building, using or interested in eBPF as a platform.

Register here

Join Summit Slack



ISOVALENT

Thank you

cilium/tetragon

@ciliumproject

isovalent.com

@lizrice