Cloud_Native Rejekts [NA'22]

October 23, 2022
Detroit, Michigan

Detecting Cryptocurrency Mining With eBPF

Tracy P Holmes

Technical Community Advocate
Isovalent

ISOVALENT

Detecting Cryptocurrency Mining With eBPF

Tracy P Holmes | @tracypholmes
Technical Community Advocate, Isovalent

ISOVALENT

Discovery Talk

ISOVALENT

Tetragon

Security Observability & Runtime Enforcement

CLOUD NATIVE COMPUTING FOUNDATION

Metrics

Events

SIEM

fluentd

Logs

Traces

JSON

Tetragon Agent

Kernel Runtime

Smart Collector

Stack Traces

Ring Buffer

Metrics

Hash Maps

Linux Kernel

Process Execution

Syscall Activity

System Calls

File Access

VFS

Seq Attack

TCP/IP

NS Escapes

Priv Escalations

Namespaces

Data Access

Storage

HTTP, DNS, TLS

Network

@tracypholmes

ISOVALENT

What activity do we care about?

- Network traffic
  - process_connect, process_close, process_accept, process_listen
- File & I/O activity
  - file_create, file_read, file_write, file_delete
- Running executables
  - process_exec, process_exit
- System call activity
  - kprobes, tracepoints and kernel function: process_kprobe (TracingPolicy)
- Changing privileges & namespace boundaries
  - caps (effective, permitted, inherited) and ns (pid, net, mnt, uts, ipc, user etc.)

ISOVALENT

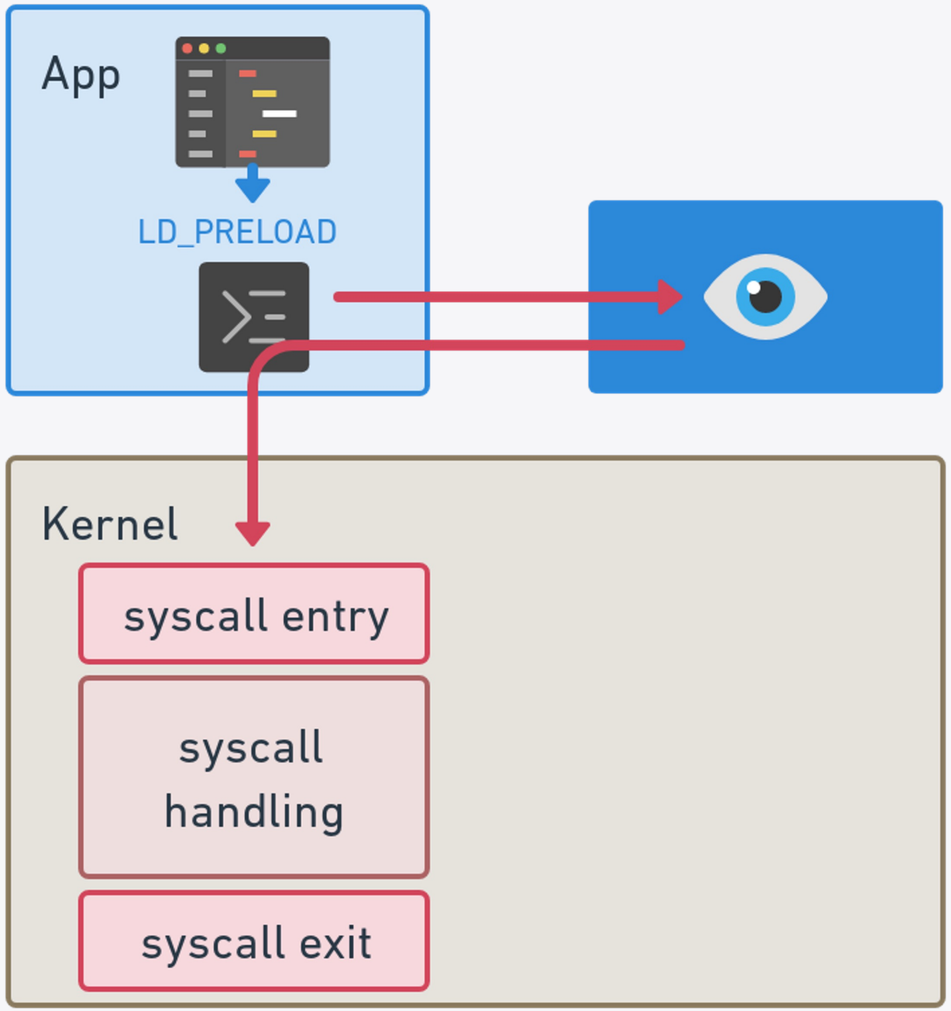
How could we spot this activity?

- LD_PRELOAD
- ptrace
- seccomp
- LSM
- eBPF - Tetragon

@tracypholmes

ISOVALENT

LD_PRELOAD

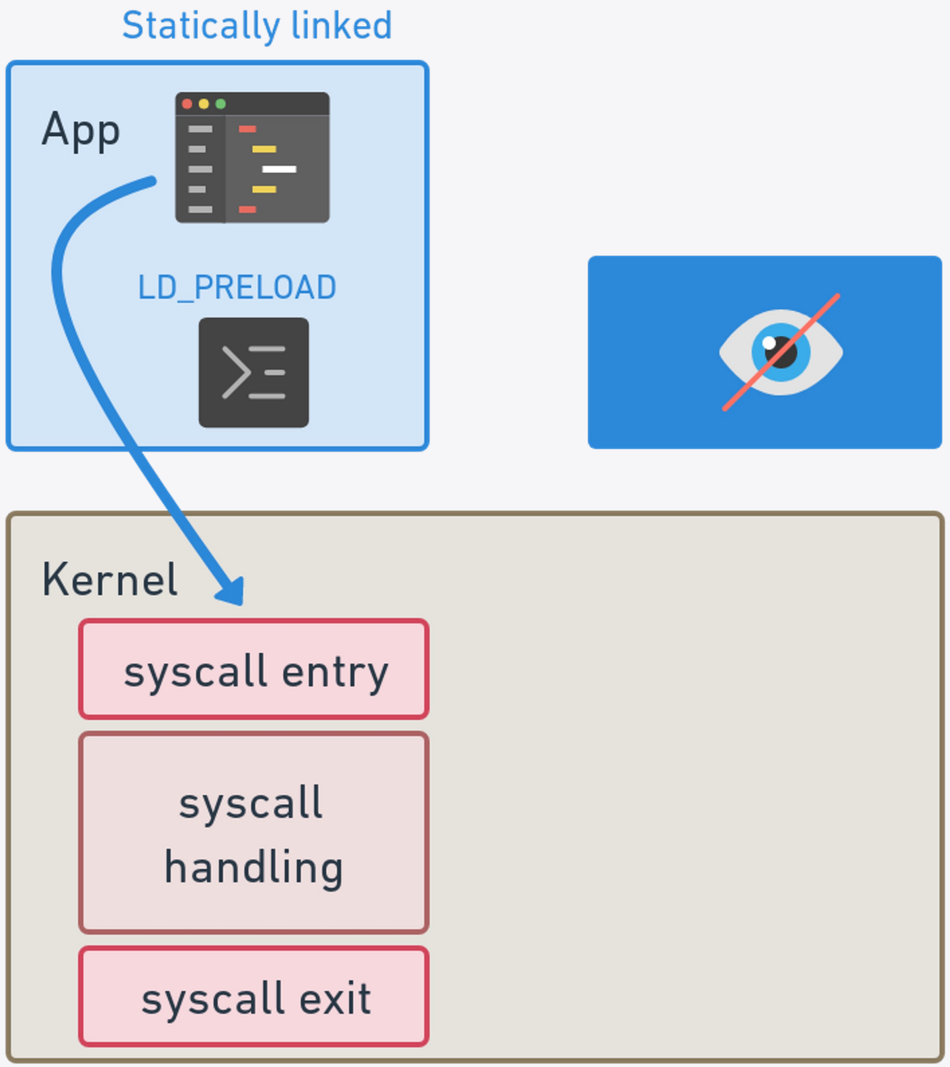


- Standard C library, dynamically linked
- System call API
- Replace the “standard” library

@tracypholmes

ISOVALENT

LD_PRELOAD

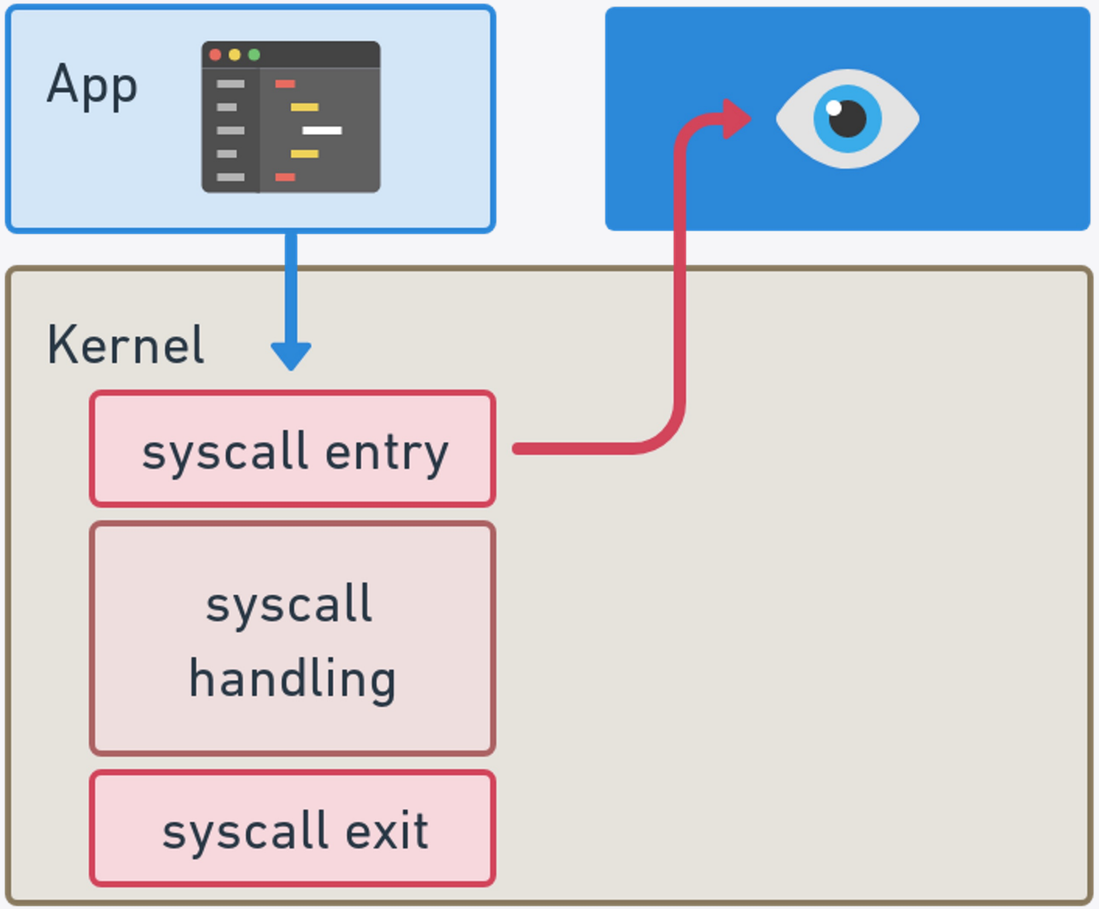


- Standard C library, dynamically linked
- System call API
- Replace the “standard” library
- **Bypassed by statically linked executables**

@tracypholmes

ISOVALENT

Syscall checks within the kernel



ptrace,

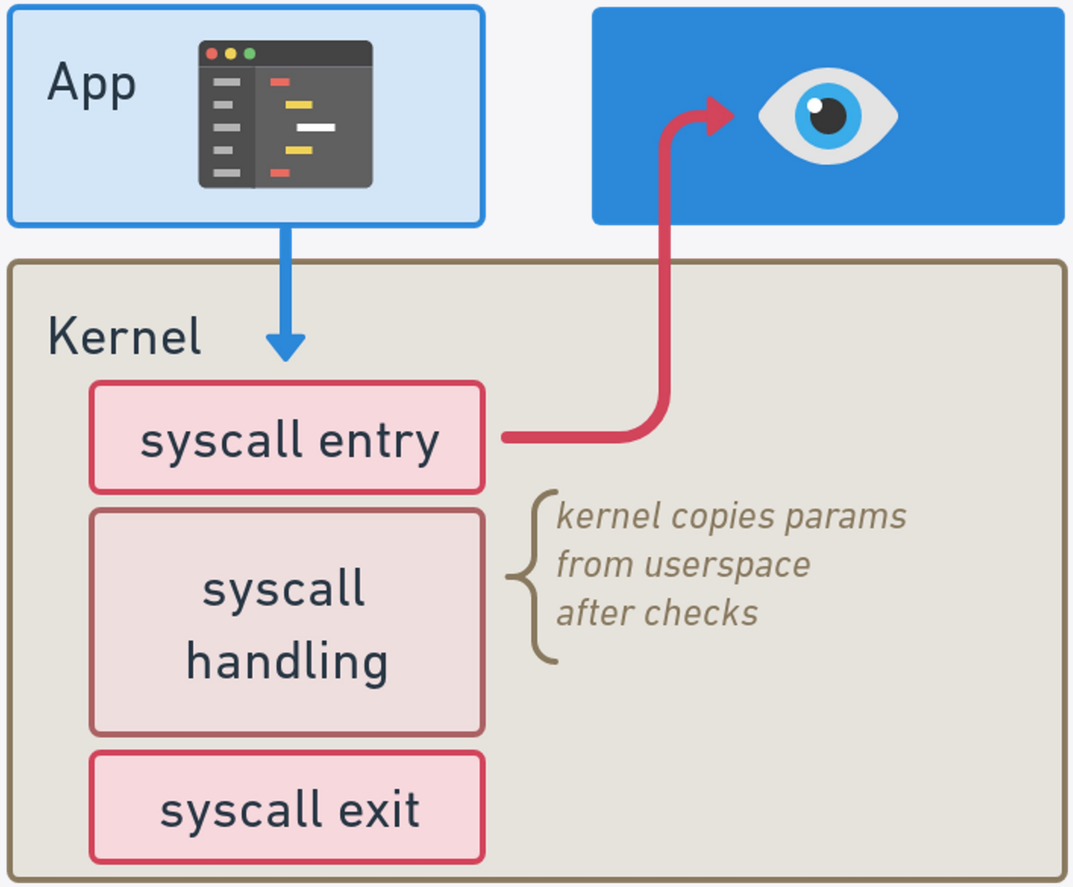
seccomp,

eBPF kprobes on syscall entry

@tracypholmes

ISOVALENT

TOCTOU with syscalls



ptrace,

seccomp,

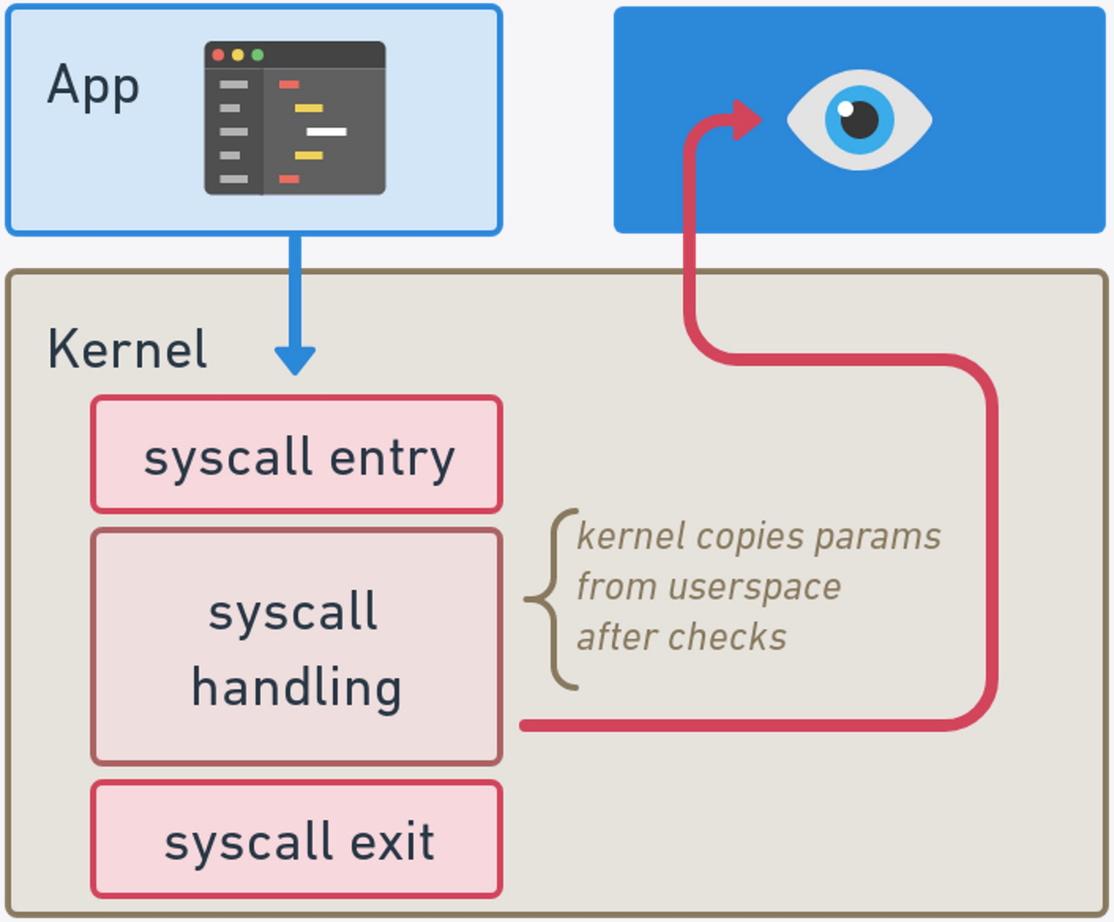
eBPF kprobes on syscall entry

For more details

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

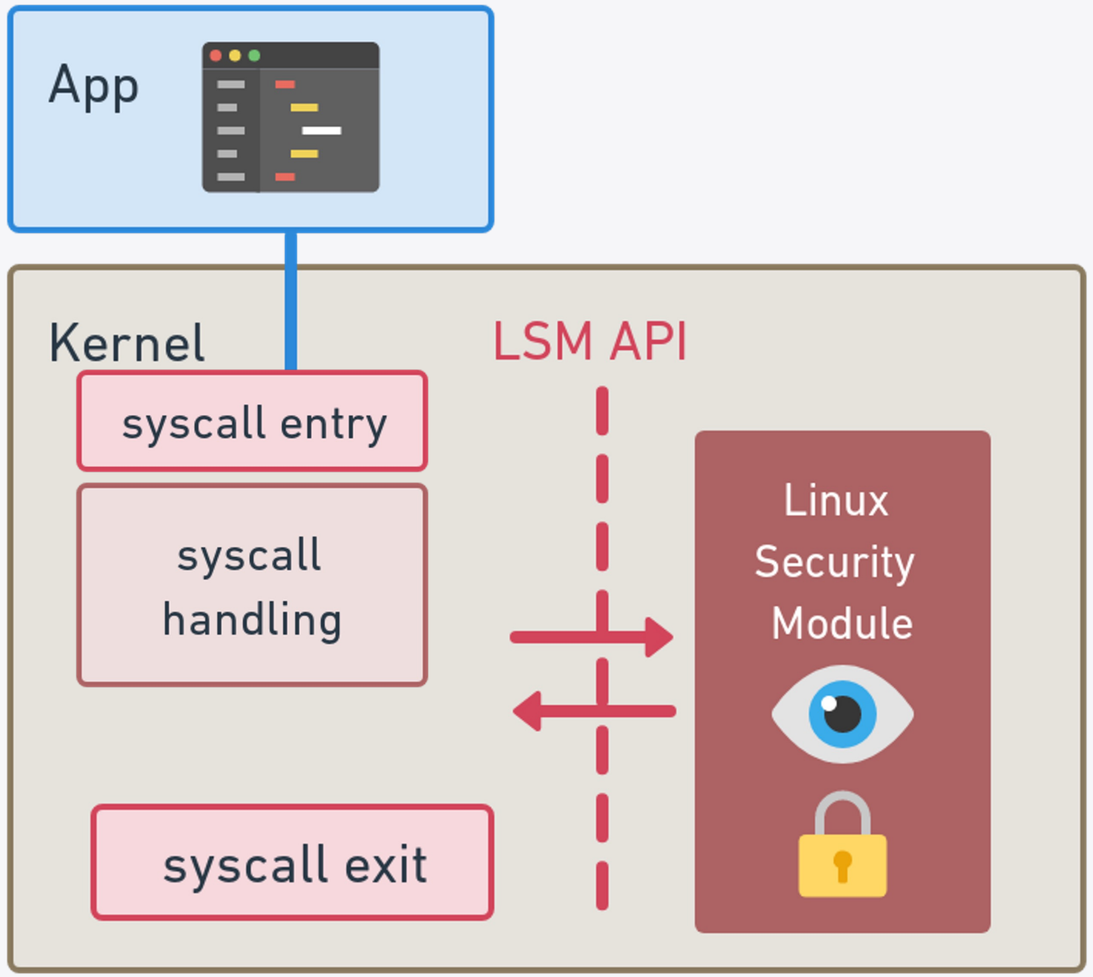
@tracypholmes

Need to make the check at the right place



ISOVALENT

Linux Security Modules

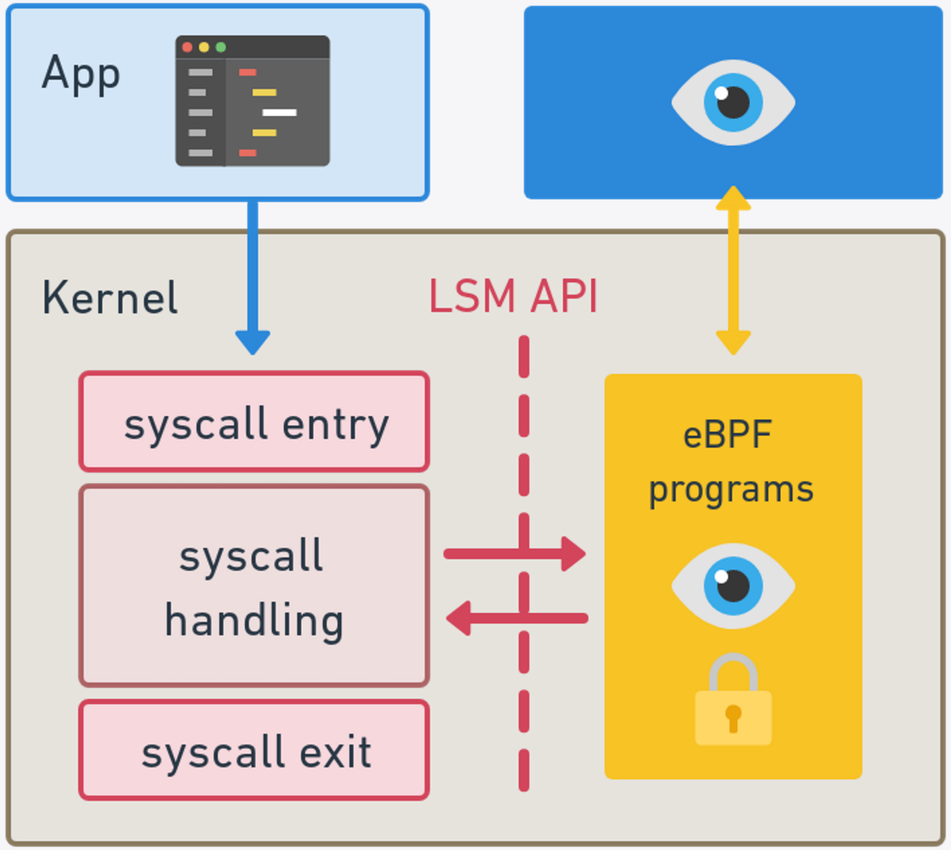


- Stable interface
- Safe places to make checks

@tracypholmes

ISOVALENT

BPF LSM

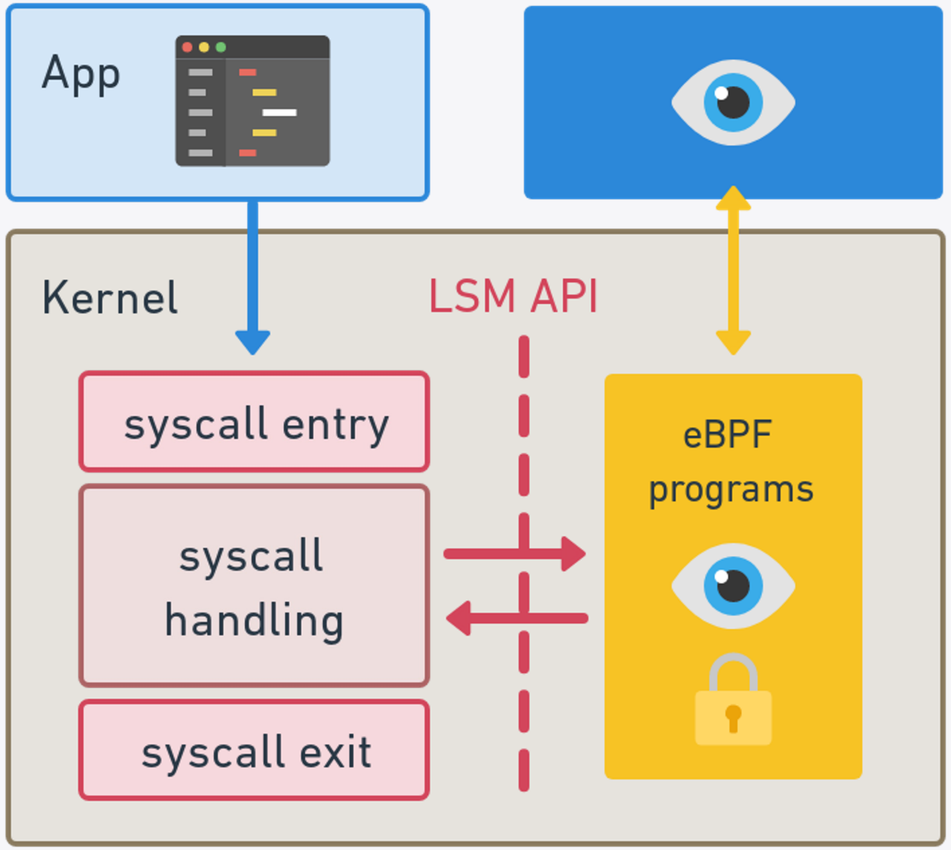


- Stable interface
- Safe places to make checks
- eBPF makes it dynamic
- Protect pre-existing processes

@tracypholmes

ISOVALENT

BPF LSM

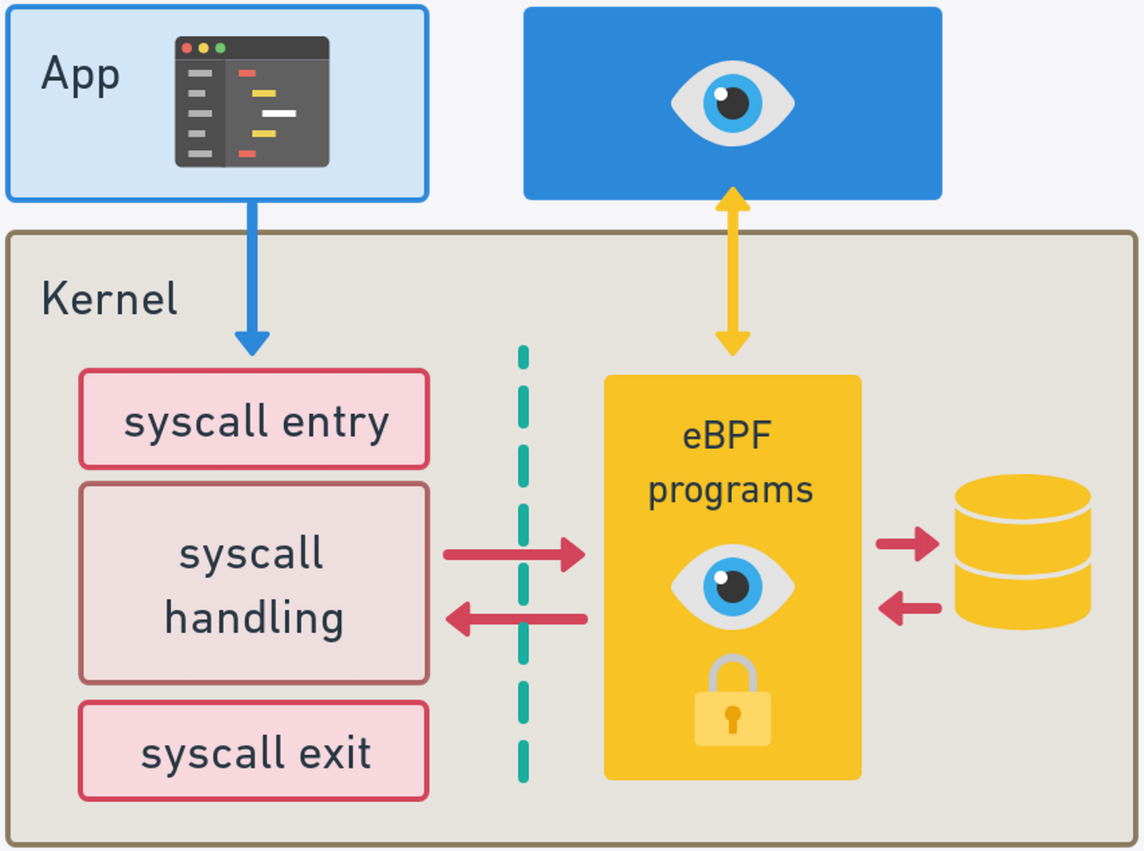


- Stable interface
- Safe places to make checks
- eBPF makes it dynamic
- Protect pre-existing processes
- Needs **kernel 5.7+**

@tracypholmes

ISOVALENT

Cilium Tetragon

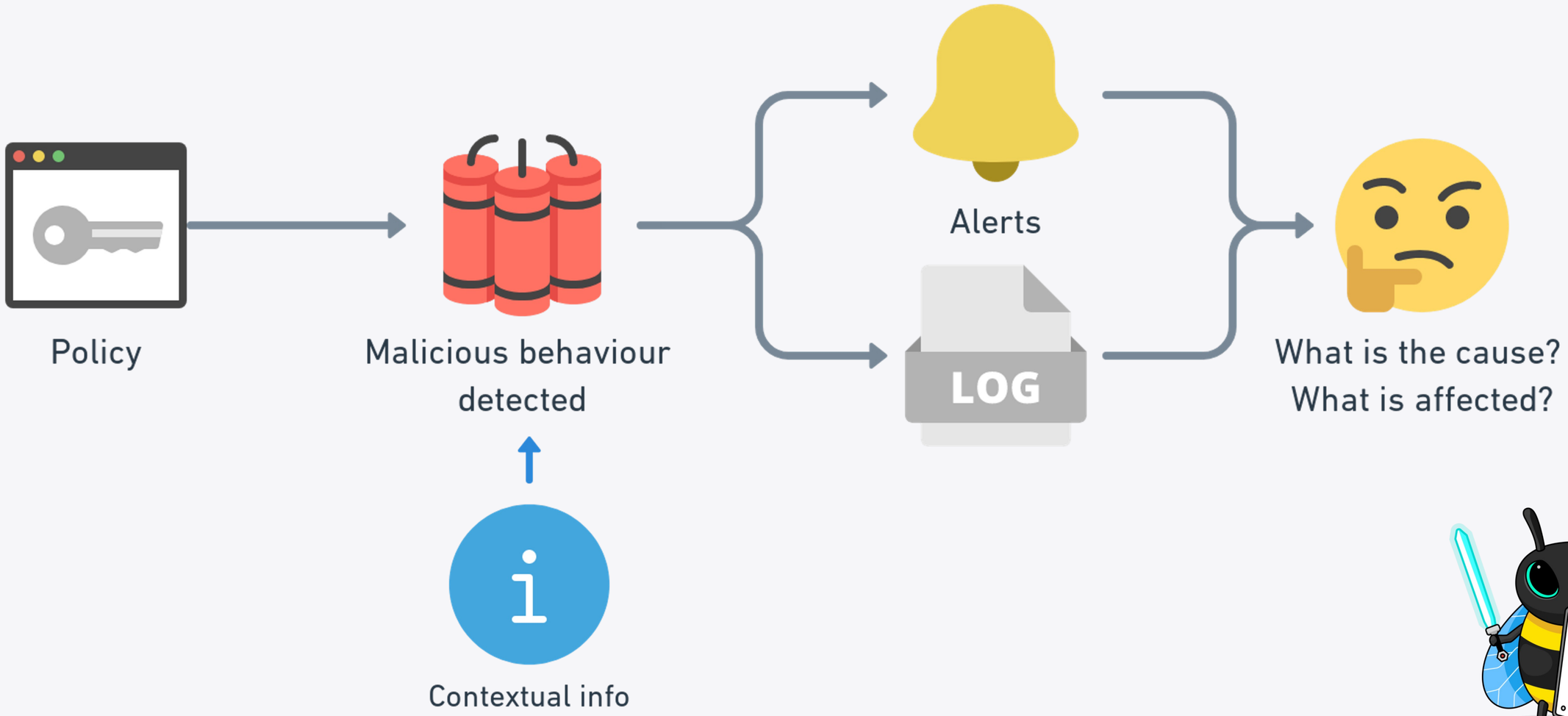


- eBPF makes it dynamic
- Protect pre-existing processes
- Uses **kernel knowledge** to hook into sufficiently stable functions
- Multiple **co-ordinated** eBPF programs
- In-kernel event **filtering**

@tracypholmes

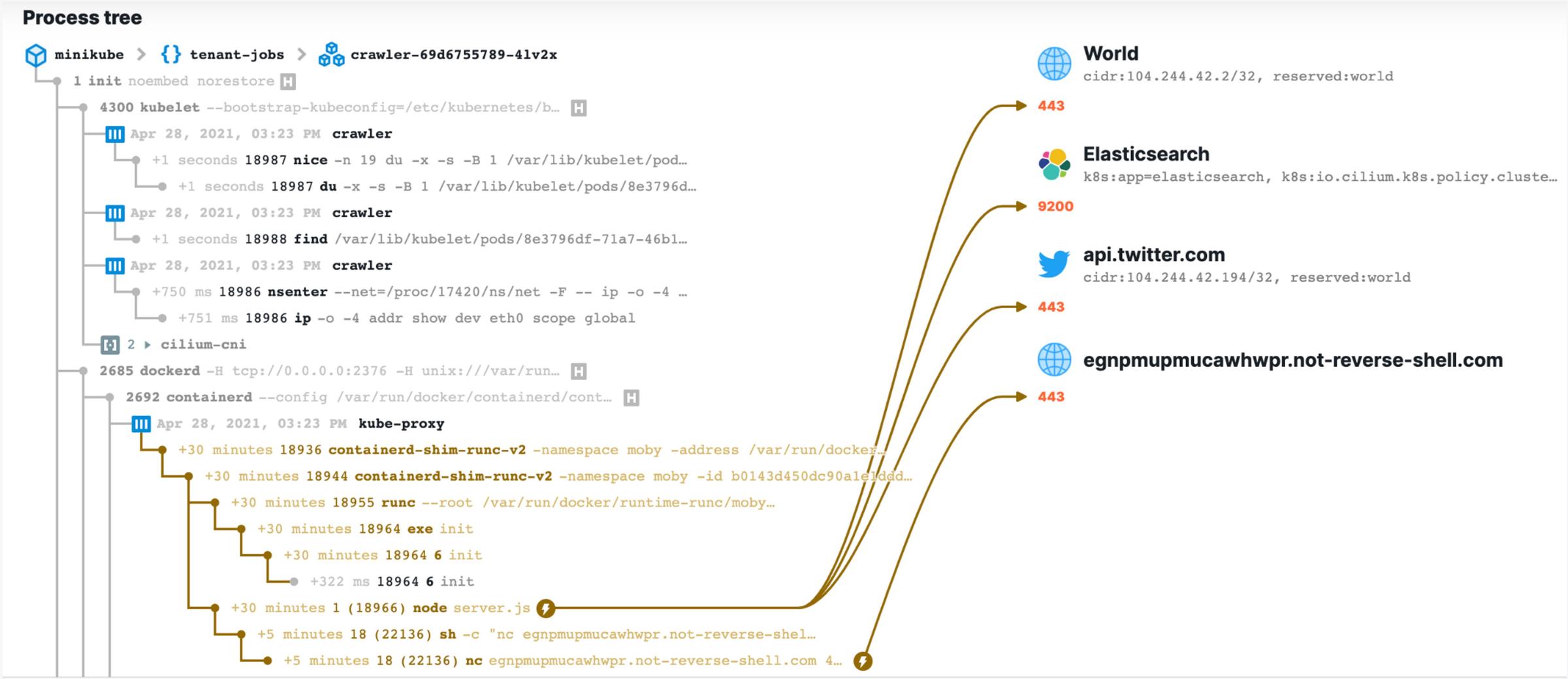
ISOVALENT

Context is everything



@tracypholmes

Combined Network & Runtime Visibility



@tracypholmes

Observing Applications & Connections

```
🚀 process default/test-pod /usr/local/bin/curl cilium.io
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.default.svc.cluster.local.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.default.svc.cluster.local.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.default.svc.cluster.local.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.default.svc.cluster.local.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.svc.cluster.local.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.svc.cluster.local.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.svc.cluster.local.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.svc.cluster.local.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.cluster.local.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.cluster.local.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.cluster.local.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.cluster.local.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.c.cilium-dev.internal.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.c.cilium-dev.internal.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.c.cilium-dev.internal.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.c.cilium-dev.internal.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.google.internal.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.google.internal.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.google.internal.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.google.internal.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.] => [104.198.14.52]
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.] => []
🔌 connect default/test-pod /usr/local/bin/curl TCP 10.80.0.12:43278 => 104.198.14.52:80 [cilium.io.]
🌐 http    default/test-pod /usr/local/bin/curl cilium.io GET / 301 Moved Permanently 154.733717ms
💥 exit    default/test-pod /usr/local/bin/curl cilium.io 0
🧹 close   default/test-pod /usr/local/bin/curl TCP 10.80.0.12:43278 => 104.198.14.52:80 [cilium.io.] tx 73 B rx 1.2 kB
🧱 socket  default/test-pod /usr/local/bin/curl TCP 10.80.0.12:43278 => 104.198.14.52:80 [cilium.io.] tx 73 B rx 1.2 kB
```

@tracypholmes

ISOVALENT

Preventing Sensitive File Access

```
process default/test-pod /usr/bin/vi /etc/shadow
open    default/test-pod /usr/bin/vi /etc/shadow
close   default/test-pod /usr/bin/vi /etc/shadow
open    default/test-pod /usr/bin/vi /etc/shadow
close   default/test-pod /usr/bin/vi /etc/shadow
open    default/test-pod /usr/bin/vi /etc/shadow
write   default/test-pod /usr/bin/vi /etc/shadow 501 bytes
exit    default/test-pod /usr/bin/vi /etc/shadow SIGKILL
```

```
    values:
    - 1
  matchArgs:
  - index: 0
    operator: "Prefix"
    values:
    - "/root/.ssh/authorized_keys"
  matchActions:
  - action: Sigkill
```

@tracypholmes

ISOVALENT

Demo Gremlins

```
~
❯ kubectl logs -n kube-system -l app.kubernetes.io/name=tetragon -c export-stdout -f | tetra getevents -o compact
^C

~                                                                                                    ✘ INT
❯ kubectl logs -n kube-system -l app.kubernetes.io/name=tetragon -c export-stdout -f
^C

~
❯ kubectl get pods -n kube-system
NAME                                      READY   STATUS             RESTARTS        AGE
cilium-operator-7b5b55f786-h9l5m          1/1     Running            0               50m
metrics-server-668d979685-tjk45           1/1     Running            0               53m
coredns-b96499967-2jrzr                   1/1     Running            0               53m
local-path-provisioner-7b7dc8d6f5-bz22k   1/1     Running            0               53m
cilium-6hhlx                              1/1     Running            0               18m
hubble-relay-768858c54c-gzs78             1/1     Running            0               18m
tetragon-xktmq                            1/2     CrashLoopBackOff   6 (4m15s ago)   10m

~
❯ kubectl describe pod -n kube-system tetragon-xktmq
Name:         tetragon-xktmq
Namespace:    kube-system
Priority:     0
Node:         lima-rancher-desktop/192.168.5.15
Start Time:   Sun, 23 Oct 2022 14:54:25 -0400
Labels:       app.kubernetes.io/instance=tetragon
              app.kubernetes.io/managed-by=Helm
              app.kubernetes.io/name=tetragon
              controller-revision-hash=6696f57647
              helm.sh/chart=tetragon-0.8.3
              pod-template-generation=1
Annotations:  <none>
Status:       Running
IP:           192.168.5.15
IPs:
```

Currently, Tetragon doesn't support ARM. However, this is in the works.

Tetragon GitHub

Issue #487

@tracypholmes

ISOVALENT

Demo Gremlins

```
                    node.kubernetes.io/unschedulable:NoSchedule op=Exists
Events:
  Type     Reason     Age                  From               Message
  ----     ------     ----                 ----               -------
  Normal   Scheduled  11m                  default-scheduler  Successfully assigned kube-system/tetragon-xktmq to lima-rancher-desktop
  Normal   Pulling    11m                  kubelet            Pulling image "quay.io/cilium/tetragon-operator:v0.8.3"
  Normal   Created    11m                  kubelet            Created container tetragon-operator
  Normal   Started    11m                  kubelet            Started container tetragon-operator
  Normal   Pulled     11m                  kubelet            Successfully pulled image "quay.io/cilium/tetragon-operator:v0.8.3" in 1.478592s
  Normal   Pulling    11m                  kubelet            Pulling image "quay.io/cilium/hubble-export-stdout:v1.0.2"
  Normal   Pulling    11m                  kubelet            Pulling image "quay.io/cilium/tetragon:v0.8.3"
  Normal   Pulled     11m                  kubelet            Successfully pulled image "quay.io/cilium/hubble-export-stdout:v1.0.2" in 894.6774
  Normal   Created    11m                  kubelet            Created container export-stdout
  Normal   Started    11m                  kubelet            Started container export-stdout
  Normal   Pulled     11m                  kubelet            Successfully pulled image "quay.io/cilium/tetragon:v0.8.3" in 3.810068336s
  Warning  Unhealthy  11m                  kubelet            Liveness probe errored: rpc error: code = Unknown desc = failed to exec in contai
ntainer is in CONTAINER_EXITED state
  Normal   Created    10m (x3 over 11m)    kubelet            Created container tetragon
  Normal   Started    10m (x3 over 11m)    kubelet            Started container tetragon
  Normal   Pulled     10m (x3 over 11m)    kubelet            Container image "quay.io/cilium/tetragon:v0.8.3" already present on machine
  Warning  BackOff    71s (x51 over 11m)   kubelet            Back-off restarting failed container
```

@tracypholmes

Resources

- eCHO episode #54 - Tetragon w/ Natália Ivánkó (with demo!)
  - https://youtu.be/vVFg8WkaeeM
- eCHO (eBPF & Cilium Office Hours)
  - https://www.youtube.com/@eBPFCilium
- Tetragon Setup
  - https://github.com/cilium/tetragon
- Pixie blog post
  - Detecting Monero miners with bpftrace | Pixie Labs Blog (px.dev)

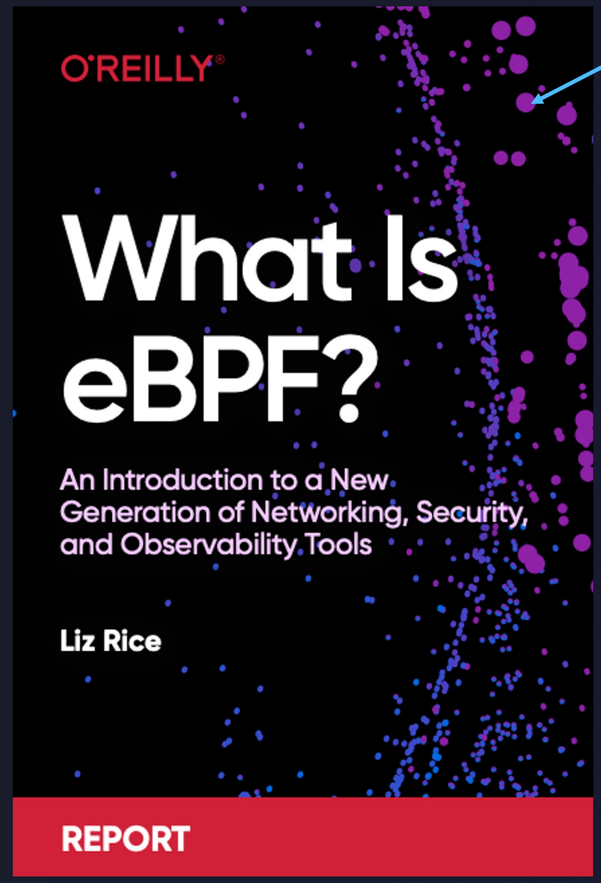
ISOVALENT

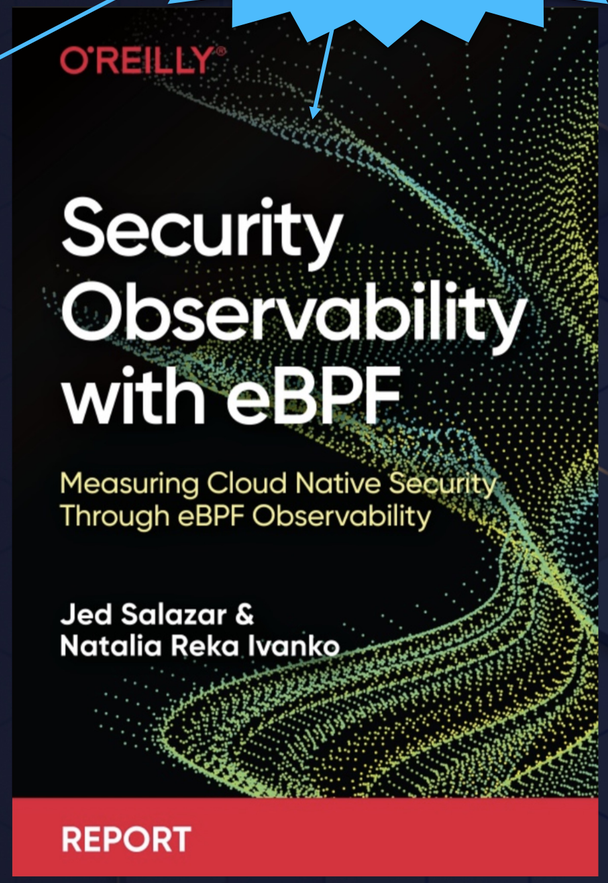
Thank you

cilium/cilium

@ciliumproject

cilium.io





Download from **isovalent.com**

@tracypholmes