Suricata QA

What/When and How

Suricata QA

- A process
  - build entirely on Open Source or free tools and services
  - in charge of 490K lines of code
  - mostly automated
    - except for specific/particular verifications
  - Using Github and Redmine for
    - bug and feature report
    - pull requests (pr) - fixes/features

Suricata QA

- Where tests can run for
  - Hours
  - Days

```
root     31737  0.0  0.0  53236 10360 pts/2    S+   Nov03   1:36 /usr/bin/perl -w /home/pmanev/
so/sid-pcap/* -c=/home/sandnet/bin/ruleset_load/suricata.sandnet.socket.yaml -e=0.05 -p=/opt/su
logs/ -N=1 -S=/opt/suricata-git-rctests/etc/suricata/rules/events-allenabled.rules -v=memcheck
root@resuricata01:~#
root@resuricata01:~# date
Sun Nov  6 07:36:09 EST 2016
```

  - Months
    - some AFL tests are running for 40+ days

GtiHub
for source management

- Well defined and publicly available criteria for pull request(PR) submission – potential change.
- PRs gets merged only upon:
  - Passing the initial/first auto test run
  - Passing all/any relevant tests
  - Core team members review
  - Fulfilled code quality submission criteria
  - RFC alignment is referenced wherever necessary

QA runs

- Per PR
- Per OS
- Per architecture
- Functional and nonfunctional checks
- Live traffic/static(pcap) processing
- Mem leak/Fuzzing
- Daily, 24/7 and/or on demand triggered

QA runs on OS
(and sub releases of those)

- Debian
- Ubuntu
- CentOS
- Fedora
- OpenSUSE

- Windows
- OpenBSD
- FreeBSD
- Hardened BSD

QA runs on architectures

- Configure
- Build
- Enabled features
- Functional / nonfunctional checks
- Fuzzing/memleaks
- PPA Package builds

- amd64
- ARM ARMv8 (arm64)
- ARM ARMv7 Soft Float (armel)
- ARM ARMv7 Hard Float (armhf)
- i386
- PowerPC64 Little-Endian (ppc64el)

QA runs
Functional checks

- Logging/stats
- UNIX socket
- Stream/defrag/reassembly
- Rulesets validation
- Rule reload
- Unittests/distcheck/coccinelle
- Configure and compile options and mixture

QA runs non-functional checks

- Performance has 4 impacting variables:
  - HW
  - Suricata version
  - Rules
  - Type of traffic
  - lock 3 and experiment with the 4th
- Memleaks/Fuzzing
- Test runs on different OS/Kernel versions

QA runs - live traffic

- Live Traffic
  - Auto rotating runs
  - different multi petter matcher algorithms
  - captured methods(mixture) with logging statistics
  - Automatic notification on err/crashes

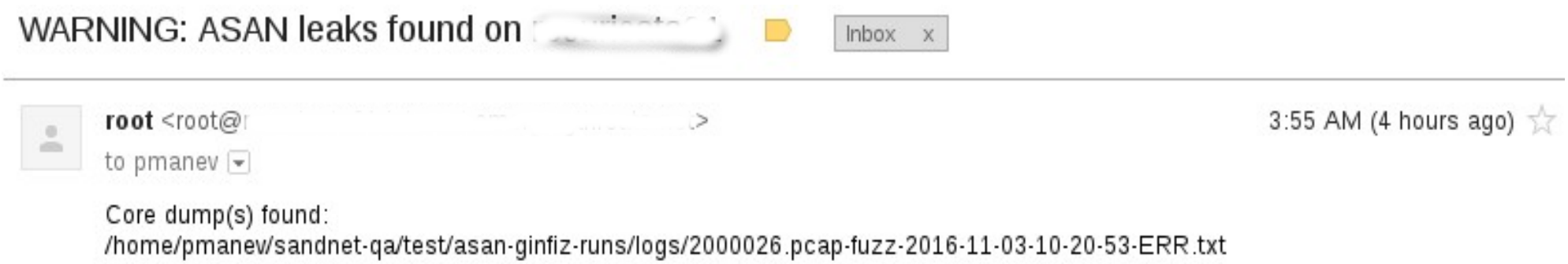
QA runs - live traffic

```
elif [ "${date_num}" == "Thu"  ]
then
  # Thursday's run
  # af+ac+custom+spm-bm+full
  # verified
  /usr/local/bin/suricata -c /etc/suricata/regit-yaml/suricata.yaml \
--pidfile /var/run/suricata.pid \
--af-packet=eth2 --af-packet=eth3 --af-packet=eth0 \
--set "af-packet.0.tpacket-v3=no" \
--set "mpm-algo=ac" --set "spm-algo=bm" --set "detect.profile=custom" \
--set "detect.custom-values.toclient-groups=700" \
--set "detect.custom-values.toserver-groups=1000" \
--set "detect.sgh-mpm-context=full" -vvv -D

elif [ "${date_num}" == "Fri"  ]
then
  # Friday's run

  # af+ac-ks+spm-bm+custom+full+eth0 on afpv3 rest afpv2 (mix af-packet)
  # verified
  /usr/local/bin/suricata -c /etc/suricata/regit-yaml/suricata.yaml \
--pidfile /var/run/suricata.pid \
--af-packet=eth2 --af-packet=eth3 --af-packet=eth0 \
--set "mpm-algo=ac-ks" --set "spm-algo=bm" --set "detect.profile=custom" \
--set "detect.custom-values.toclient-groups=700" \
--set "detect.custom-values.toserver-groups=1000" \
--set "detect.sgh-mpm-context=full" \
--set "af-packet.0.use-mmap=yes" --set "af-packet.0.mmap-locked=yes" \
--set "af-packet.0.tpacket-v3=yes" -vvv -D

elif [ "${date_num}" == "Sat"  ]
then
  # Saturday's run
  # af+hs+high+single
  # full takes a lot fo time to load (bug on redmine #1770)
  # verified
  /usr/local/bin/suricata -c /etc/suricata/regit-yaml/suricata.yaml \
--pidfile /var/run/suricata.pid \
--af-packet=eth2 --af-packet=eth3 --af-packet=eth0 \
--set "af-packet.0.tpacket-v3=no" \
--set "mpm-algo=hs" --set "spm-algo=hs" --set "detect.profile=high" \
--set "detect.sgh-mpm-context=single" -vvv -D
```

```
016-10-04.log  stats-2016-10-29.log     suricata-2016-07-29.log
016-10-05.log  stats-2016-10-30.log     suricata-2016-07-30.log
016-10-06.log  stats-2016-10-31.log     suricata-2016-07-31.log
016-10-07.log  stats-2016-11-01.log     suricata-2016-08-01.log
016-10-08.log  stats-2016-11-02.log     suricata-2016-08-02.log
016-10-09.log  stats-2016-11-03.log     suricata-2016-08-03.log
016-10-10.log  stats-2016-11-04.log     suricata-2016-08-04.log
016-10-11.log  stats-2016-11-05.log     suricata-2016-08-05.log
016-10-12.log  suricata-2016-07-12.log  suricata-2016-08-06.log
016-10-13.log  suricata-2016-07-13.log  suricata-2016-08-07.log
016-10-14.log  suricata-2016-07-14.log  suricata-2016-08-08.log
016-10-15.log  suricata-2016-07-15.log  suricata-2016-08-09.log
016-10-16.log  suricata-2016-07-16.log  suricata-2016-08-10.log
016-10-17.log  suricata-2016-07-17.log  suricata-2016-08-11.log
016-10-18.log  suricata-2016-07-18.log  suricata-2016-08-12.log
016-10-19.log  suricata-2016-07-19.log  suricata-2016-08-13.log
016-10-20.log  suricata-2016-07-20.log  suricata-2016-08-14.log
016-10-21.log  suricata-2016-07-21.log  suricata-2016-08-15.log
016-10-22.log  suricata-2016-07-22.log  suricata-2016-08-16.log
016-10-23.log  suricata-2016-07-23.log  suricata-2016-08-17.log
016-10-24.log  suricata-2016-07-24.log  suricata-2016-08-18.log
016-10-25.log  suricata-2016-07-25.log  suricata-2016-08-19.log
016-10-26.log  suricata-2016-07-26.log  suricata-2016-08-20.log
016-10-27.log  suricata-2016-07-27.log  suricata-2016-08-21.log
016-10-28.log  suricata-2016-07-28.log  suricata-2016-08-22.log
```

QA runs static traffic

- Static Traffic
  - Automatic notification when running on live boxes on mem leaks fuzzing on pcaps
  - Can be thousands of pcap runs a day with unix socket



Ubuntu PPA Launchpad packaging

- Produces 32/64/armhf/ppc64el deb packages
- For all officially supported Ubuntu releases
- Packages for
  - Suricata stable
  - Suricata beta/RC
  - Suricata daily (git)

QA Ubuntu PPA Launchpad packaging

Status	When complete	Distribution series	Archive
Successful build	2 hours ago buildlog (11.6 KiB)	Xenial	suricata-daily-allarch
suricata - 201611022033+f9f5e8a~ubuntu16.04.1	2 hours ago buildlog (29.5 KiB)	amd64	
suricata - 201611022033+f9f5e8a~ubuntu16.04.1	2 hours ago buildlog (29.4 KiB)	arm64	
suricata - 201611022033+f9f5e8a~ubuntu16.04.1	2 hours ago buildlog (29.3 KiB)	armhf	
suricata - 201611022033+f9f5e8a~ubuntu16.04.1	2 hours ago buildlog (29.4 KiB)	i386	
suricata - 201611022033+f9f5e8a~ubuntu16.04.1	2 hours ago buildlog (29.4 KiB)	ppc64el	
Successful build	2 hours ago buildlog (8.3 KiB)	Yakkety	suricata-daily-allarch
suricata - 201611022031+f9f5e8a~ubuntu16.10.1	2 hours ago buildlog (26.1 KiB)	amd64	
suricata - 201611022031+f9f5e8a~ubuntu16.10.1	2 hours ago buildlog (26.1 KiB)	arm64	
suricata - 201611022031+f9f5e8a~ubuntu16.10.1	2 hours ago buildlog (26.1 KiB)	armhf	
suricata - 201611022031+f9f5e8a~ubuntu16.10.1	2 hours ago buildlog (26.1 KiB)	i386	
suricata - 201611022031+f9f5e8a~ubuntu16.10.1	2 hours ago buildlog (26.1 KiB)	ppc64el	
Successful build	2 hours ago buildlog (10.0 KiB)	Zesty	suricata-daily-allarch
suricata - 201611022032+f9f5e8a~ubuntu17.04.1	2 hours ago buildlog (27.9 KiB)	amd64	
suricata - 201611022032+f9f5e8a~ubuntu17.04.1	2 hours ago buildlog (27.7 KiB)	arm64	
suricata - 201611022032+f9f5e8a~ubuntu17.04.1	2 hours ago buildlog (27.7 KiB)	armhf	
suricata - 201611022032+f9f5e8a~ubuntu17.04.1	2 hours ago buildlog (27.9 KiB)	i386	
suricata - 201611022032+f9f5e8a~ubuntu17.04.1	2 hours ago buildlog (27.8 KiB)	ppc64el	
Successful build	2 hours ago buildlog (13.2 KiB)	Precise	suricata-daily-allarch
suricata - 201611022031+f9f5e8a~ubuntu12.04.1	2 hours ago buildlog (26.3 KiB)	amd64	
suricata - 201611022031+f9f5e8a~ubuntu12.04.1	2 hours ago buildlog (26.3 KiB)	armhf	
suricata - 201611022031+f9f5e8a~ubuntu12.04.1	2 hours ago buildlog (26.3 KiB)	i386	
Successful build	2 hours ago buildlog (13.1 KiB)	Trusty	suricata-daily-allarch
suricata - 201611022031+f9f5e8a~ubuntu14.04.1	2 hours ago buildlog (26.0 KiB)	amd64	
suricata - 201611022031+f9f5e8a~ubuntu14.04.1	2 hours ago buildlog (26.0 KiB)	arm64	

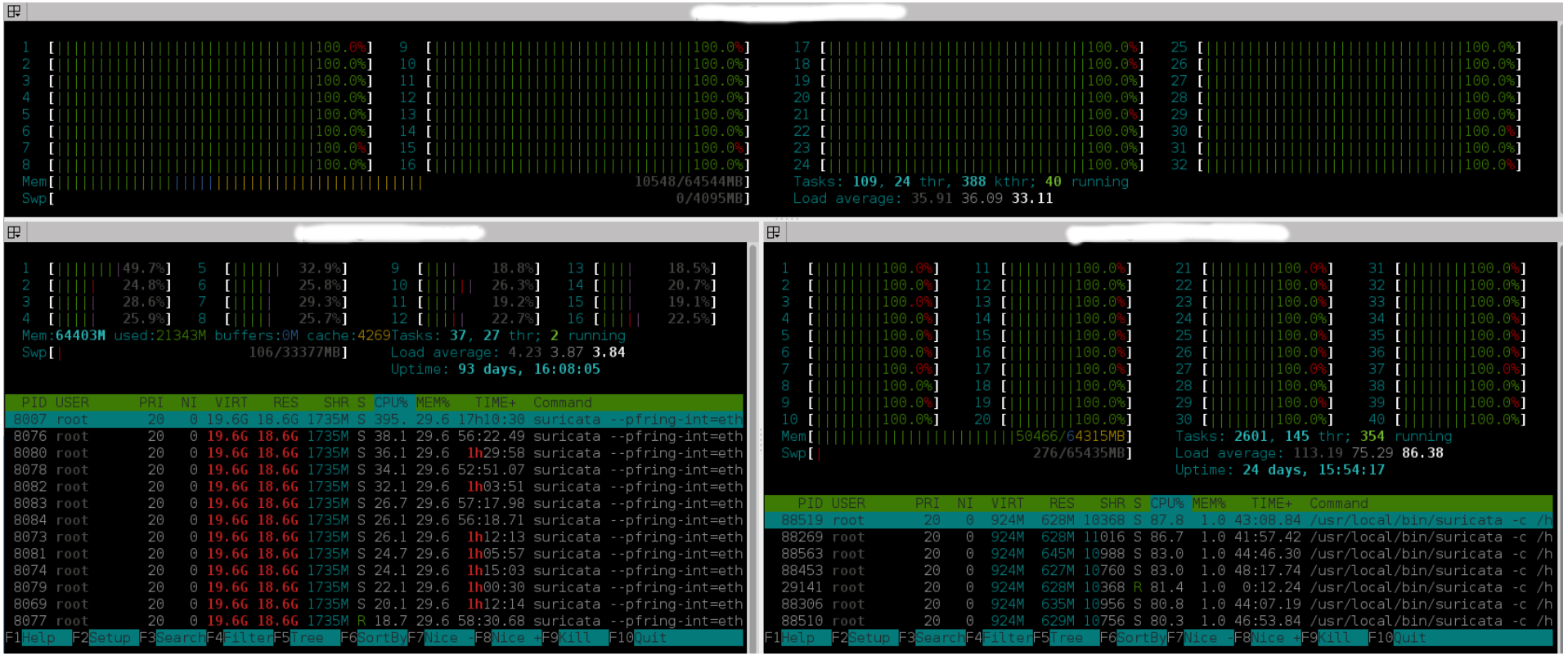
QA Ubuntu PPA Launchpad packaging

- Packages are tested for
  - Install/upgrade
  - Unix socket
  - Live rule reloads
  - Alerting/logs
  - Correct version dependencies
  - Features enabled

24/7 QA runs

- Memleaks/AFL
  - ASAN/UBSan/Valgrind
- Pcap fuzzing
  - Valid and purposefully malformed pcaps
- Live traffic
- Capture methods
- Memory algorithms

24/7 QA runs

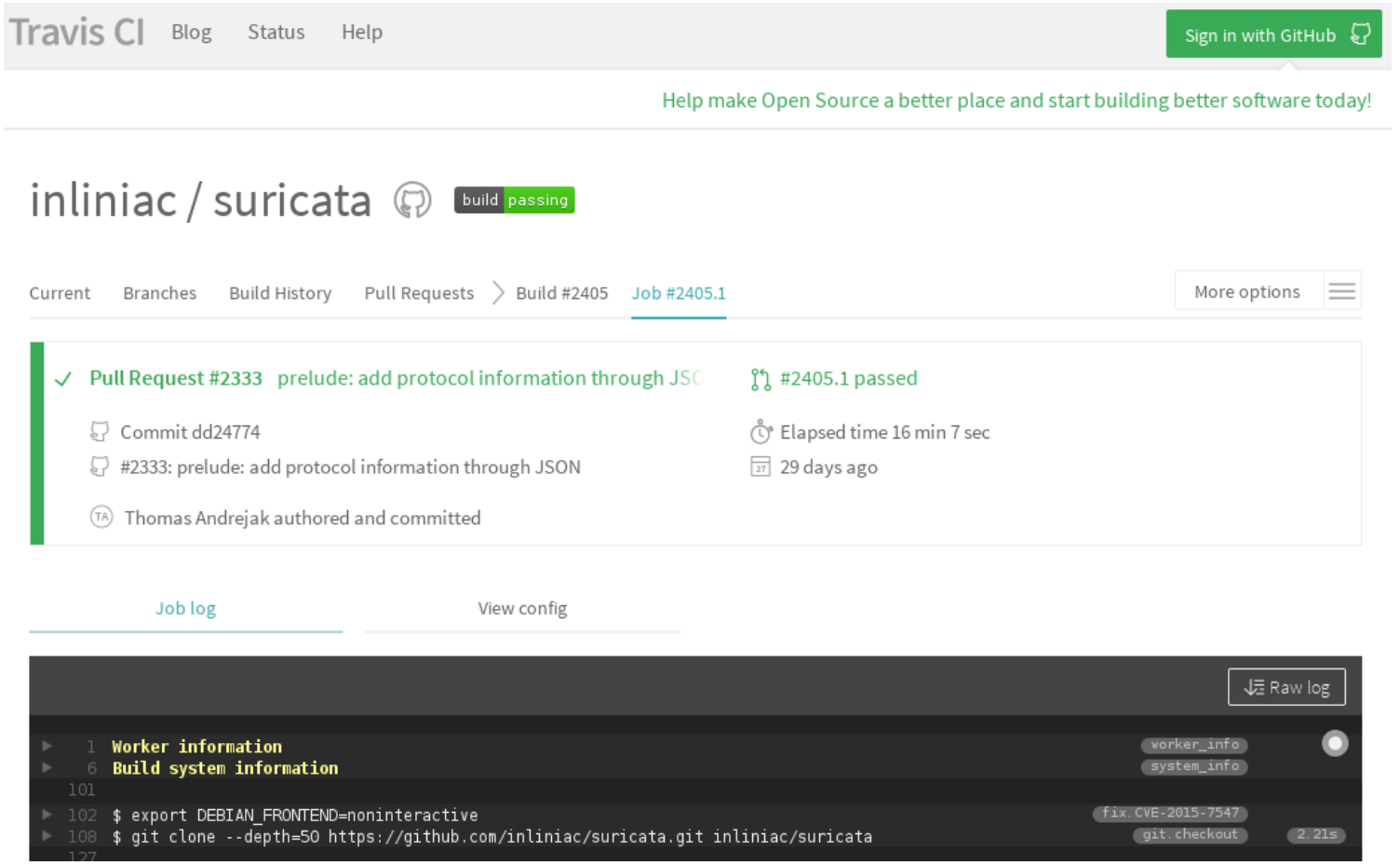


SURIQA

Major tools/systems used

- Travis CI
- Buildbot (Per OS including BSD and win)
- Docker (per OS/OS release)
- Github
- Gitlab
- Perf top/perf report/perf stat suite
- Asan/UBSan/Valgrind
- AFL/pcap (fuzzing)
- Coverty scan
- Intel Perf counter monitor
- Pcap runs
- Live traffic boxes
- iperf

Travis CI/Github



QA Challenges

- Centralization
- Privacy of pcaps/reports
- Arsenal of different tools and systems
- Lots of HW vendor (NIC/arch) to cover

Big THANK YOU to Suricata community for reporting bugs!

THANK YOU

SURICON

SURIQA

SURICATA