

Suricata QA

What/When and How



SURIQA



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/suricata-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
116-10-04.log stats-2016-10-29.log suricata-2016-07-29.log
116-10-05.log stats-2016-10-30.log suricata-2016-07-30.log
116-10-06.log stats-2016-10-31.log suricata-2016-07-31.log
116-10-07.log stats-2016-11-01.log suricata-2016-08-01.log
116-10-08.log stats-2016-11-02.log suricata-2016-08-02.log
116-10-09.log stats-2016-11-03.log suricata-2016-08-03.log
116-10-10.log stats-2016-11-04.log suricata-2016-08-04.log
116-10-11.log stats-2016-11-05.log suricata-2016-08-05.log
116-10-12.log suricata-2016-07-12.log suricata-2016-08-06.log
116-10-13.log suricata-2016-07-13.log suricata-2016-08-07.log
116-10-14.log suricata-2016-07-14.log suricata-2016-08-08.log
116-10-15.log suricata-2016-07-15.log suricata-2016-08-09.log
116-10-16.log suricata-2016-07-16.log suricata-2016-08-10.log
116-10-17.log suricata-2016-07-17.log suricata-2016-08-11.log
116-10-18.log suricata-2016-07-18.log suricata-2016-08-12.log
116-10-19.log suricata-2016-07-19.log suricata-2016-08-13.log
116-10-20.log suricata-2016-07-20.log suricata-2016-08-14.log
116-10-21.log suricata-2016-07-21.log suricata-2016-08-15.log
116-10-22.log suricata-2016-07-22.log suricata-2016-08-16.log
116-10-23.log suricata-2016-07-23.log suricata-2016-08-17.log
116-10-24.log suricata-2016-07-24.log suricata-2016-08-18.log
116-10-25.log suricata-2016-07-25.log suricata-2016-08-19.log
116-10-26.log suricata-2016-07-26.log suricata-2016-08-20.log
116-10-27.log suricata-2016-07-27.log suricata-2016-08-21.log
116-10-28.log suricata-2016-07-28.log suricata-2016-08-22.log

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
```



SURIQA



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

WARNING: ASAN leaks found on 



Inbox x



root <root@...>
to pmanev

3:55 AM (4 hours ago) ☆

Core dump(s) found:
/home/pmanev/sandnet-qa/test/asan-ginfiz-runs/logs/2000026.pcap-fuzz-2016-11-03-10-20-53-ERR.txt



SURIQA



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 suricata - 201611022033+F9F5e8a~ubuntu16.04.1 suricata - 201611022033+F9F5e8a~ubuntu16.04.1 suricata - 201611022033+F9F5e8a~ubuntu16.04.1 suricata - 201611022033+F9F5e8a~ubuntu16.04.1 suricata - 201611022033+F9F5e8a~ubuntu16.04.1	2 hours ago buildlog (11.6 KiB) 2 hours ago buildlog (29.5 KiB) 2 hours ago buildlog (29.4 KiB) 2 hours ago buildlog (29.3 KiB) 2 hours ago buildlog (29.4 KiB) 2 hours ago buildlog (29.4 KiB)	Xenial amd64 arm64 armhf i386 ppc64el	suricata-daily-allarch
Successful build suricata - 201611022031+F9F5e8a~ubuntu16.10.1 suricata - 201611022031+F9F5e8a~ubuntu16.10.1 suricata - 201611022031+F9F5e8a~ubuntu16.10.1 suricata - 201611022031+F9F5e8a~ubuntu16.10.1 suricata - 201611022031+F9F5e8a~ubuntu16.10.1	2 hours ago buildlog (8.3 KiB) 2 hours ago buildlog (26.1 KiB) 2 hours ago buildlog (26.1 KiB) 2 hours ago buildlog (26.1 KiB) 2 hours ago buildlog (26.1 KiB) 2 hours ago buildlog (26.1 KiB)	Yakkety amd64 arm64 armhf i386 ppc64el	suricata-daily-allarch
Successful build suricata - 201611022032+F9F5e8a~ubuntu17.04.1 suricata - 201611022032+F9F5e8a~ubuntu17.04.1 suricata - 201611022032+F9F5e8a~ubuntu17.04.1 suricata - 201611022032+F9F5e8a~ubuntu17.04.1 suricata - 201611022032+F9F5e8a~ubuntu17.04.1	2 hours ago buildlog (10.0 KiB) 2 hours ago buildlog (27.9 KiB) 2 hours ago buildlog (27.7 KiB) 2 hours ago buildlog (27.7 KiB) 2 hours ago buildlog (27.9 KiB) 2 hours ago buildlog (27.8 KiB)	Zesty amd64 arm64 armhf i386 ppc64el	suricata-daily-allarch
Successful build suricata - 201611022031+F9F5e8a~ubuntu12.04.1 suricata - 201611022031+F9F5e8a~ubuntu12.04.1 suricata - 201611022031+F9F5e8a~ubuntu12.04.1	2 hours ago buildlog (13.2 KiB) 2 hours ago buildlog (26.3 KiB) 2 hours ago buildlog (26.3 KiB) 2 hours ago buildlog (26.3 KiB)	Precise amd64 armhf i386	suricata-daily-allarch
Successful build suricata - 201611022031+F9F5e8a~ubuntu14.04.1 suricata - 201611022031+F9F5e8a~ubuntu14.04.1	2 hours ago buildlog (13.1 KiB) 2 hours ago buildlog (26.0 KiB) 2 hours ago buildlog (26.0 KiB)	Trusty amd64 arm64	suricata-daily-allarch



SURIQA



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

```

1 [|||||] 100.0% 9 [|||||] 100.0% 17 [|||||] 100.0% 25 [|||||] 100.0%
2 [|||||] 100.0% 10 [|||||] 100.0% 18 [|||||] 100.0% 26 [|||||] 100.0%
3 [|||||] 100.0% 11 [|||||] 100.0% 19 [|||||] 100.0% 27 [|||||] 100.0%
4 [|||||] 100.0% 12 [|||||] 100.0% 20 [|||||] 100.0% 28 [|||||] 100.0%
5 [|||||] 100.0% 13 [|||||] 100.0% 21 [|||||] 100.0% 29 [|||||] 100.0%
6 [|||||] 100.0% 14 [|||||] 100.0% 22 [|||||] 100.0% 30 [|||||] 100.0%
7 [|||||] 100.0% 15 [|||||] 100.0% 23 [|||||] 100.0% 31 [|||||] 100.0%
8 [|||||] 100.0% 16 [|||||] 100.0% 24 [|||||] 100.0% 32 [|||||] 100.0%
Mem[|||||] 10548/64544MB Tasks: 109, 24 thr, 388 kthr; 40 running
Swp[|||||] 0/4095MB Load average: 35.91 36.09 33.11
  
```

```

1 [|||||] 49.7% 5 [|||||] 32.9% 9 [|||||] 18.8% 13 [|||||] 18.5%
2 [|||||] 24.8% 6 [|||||] 25.8% 10 [|||||] 26.3% 14 [|||||] 20.7%
3 [|||||] 28.6% 7 [|||||] 29.3% 11 [|||||] 19.2% 15 [|||||] 19.1%
4 [|||||] 25.9% 8 [|||||] 25.7% 12 [|||||] 22.7% 16 [|||||] 22.5%
Mem:64403M used:21343M buffers:0M cache:4269Tasks: 37, 27 thr; 2 running
Swp[|||||] 106/33377MB Load average: 4.23 3.87 3.84
Uptime: 93 days, 16:08:05
  
```

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
8007	root	20	0	19.6G	18.6G	1735M	S	395.1	29.6	17h10:30	suricata --pfring-int=eth
8076	root	20	0	19.6G	18.6G	1735M	S	38.1	29.6	56:22.49	suricata --pfring-int=eth
8080	root	20	0	19.6G	18.6G	1735M	S	36.1	29.6	1h29:58	suricata --pfring-int=eth
8078	root	20	0	19.6G	18.6G	1735M	S	34.1	29.6	52:51.07	suricata --pfring-int=eth
8082	root	20	0	19.6G	18.6G	1735M	S	32.1	29.6	1h03:51	suricata --pfring-int=eth
8083	root	20	0	19.6G	18.6G	1735M	S	26.7	29.6	57:17.98	suricata --pfring-int=eth
8084	root	20	0	19.6G	18.6G	1735M	S	26.1	29.6	56:18.71	suricata --pfring-int=eth
8073	root	20	0	19.6G	18.6G	1735M	S	26.1	29.6	1h12:13	suricata --pfring-int=eth
8081	root	20	0	19.6G	18.6G	1735M	S	24.7	29.6	1h05:57	suricata --pfring-int=eth
8074	root	20	0	19.6G	18.6G	1735M	S	24.1	29.6	1h15:03	suricata --pfring-int=eth
8079	root	20	0	19.6G	18.6G	1735M	S	22.1	29.6	1h00:30	suricata --pfring-int=eth
8069	root	20	0	19.6G	18.6G	1735M	S	20.1	29.6	1h12:14	suricata --pfring-int=eth
8077	root	20	0	19.6G	18.6G	1735M	R	18.7	29.6	58:30.68	suricata --pfring-int=eth

F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice F8Nice F9Kill F10Quit

```

1 [|||||] 100.0% 11 [|||||] 100.0% 21 [|||||] 100.0% 31 [|||||] 100.0%
2 [|||||] 100.0% 12 [|||||] 100.0% 22 [|||||] 100.0% 32 [|||||] 100.0%
3 [|||||] 100.0% 13 [|||||] 100.0% 23 [|||||] 100.0% 33 [|||||] 100.0%
4 [|||||] 100.0% 14 [|||||] 100.0% 24 [|||||] 100.0% 34 [|||||] 100.0%
5 [|||||] 100.0% 15 [|||||] 100.0% 25 [|||||] 100.0% 35 [|||||] 100.0%
6 [|||||] 100.0% 16 [|||||] 100.0% 26 [|||||] 100.0% 36 [|||||] 100.0%
7 [|||||] 100.0% 17 [|||||] 100.0% 27 [|||||] 100.0% 37 [|||||] 100.0%
8 [|||||] 100.0% 18 [|||||] 100.0% 28 [|||||] 100.0% 38 [|||||] 100.0%
9 [|||||] 100.0% 19 [|||||] 100.0% 29 [|||||] 100.0% 39 [|||||] 100.0%
10 [|||||] 100.0% 20 [|||||] 100.0% 30 [|||||] 100.0% 40 [|||||] 100.0%
Mem[|||||] 50466/64315MB Tasks: 2601, 145 thr; 354 running
Swp[|||||] 276/65435MB Load average: 113.19 75.29 86.38
Uptime: 24 days, 15:54:17
  
```

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
88519	root	20	0	924M	628M	10368	S	87.8	1.0	43:08.84	/usr/local/bin/suricata -c /h
88269	root	20	0	924M	628M	11016	S	86.7	1.0	41:57.42	/usr/local/bin/suricata -c /h
88563	root	20	0	924M	645M	10988	S	83.0	1.0	44:46.30	/usr/local/bin/suricata -c /h
88453	root	20	0	924M	627M	10760	S	83.0	1.0	48:17.74	/usr/local/bin/suricata -c /h
29141	root	20	0	924M	628M	10368	R	81.4	1.0	0:12.24	/usr/local/bin/suricata -c /h
88306	root	20	0	924M	635M	10956	S	80.8	1.0	44:07.19	/usr/local/bin/suricata -c /h
88510	root	20	0	924M	629M	10756	S	80.3	1.0	46:53.84	/usr/local/bin/suricata -c /h

F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice F8Nice F9Kill F10Quit



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



Help make Open Source a better place and start building better software today!



inliniac / suricata  build passing


[Current](#) [Branches](#) [Build History](#) [Pull Requests](#) > [Build #2405](#) [Job #2405.1](#)

[More options](#) 

✓ [Pull Request #2333](#) prelude: add protocol information through JSON  #2405.1 passed

 Commit dd24774  Elapsed time 16 min 7 sec

 #2333: prelude: add protocol information through JSON  29 days ago

 Thomas Andrejak authored and committed

[Job log](#)

[View config](#)

```
1 Worker information worker_info
6 Build system information system_info
101
102 $ export DEBIAN_FRONTEND=noninteractive fix CVE-2015-7547
108 $ git clone --depth=50 https://github.com/inliniac/suricata.git inliniac/suricata git checkout 2.21s
127
```



SURIQA



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

