Contributing to Suricata

November 2017 -- Victor Julien, OISF

Overview

- Legal side
- Code
- Github & QA
- Post-merge

Contributors (by commit)

42 Mats Klepsland	1 Abbed
8 Pierre Chifflier	1 Derek
6 Alexander Gozman	1 Giuseppe Longo
5 David Wharton	1 Julian
5 Sascha Steinbiss	1 Peter Sanders
4 Phil Young	1 Sebastian Garcia
4 fooinha	1 Selivanov Pavel
2 Jon Zeolla	1 Travis Green
2 Ray Ruvinskiy	1 psanders240
2 jason taylor	1 qiangbei

SURICON
PRAGUE
2017

Legal

Legal

- Contrib agreement
- Makes sure OISF owns the code
- We need this to:
  - Defend Suricata in case of legal challenges
  - Reduce risk to our users (e.g. avoid netfilters current troubles)
  - Support Suricata dev through the consortium
- Contrib agreement at the website or part of custom agreements

Code

Features?

- Please probe if the team (and/or larger community) is interested in a feature before spending a lot of time on it
- We will not accept just any feature
- IRC: #suricata at freenode.net

Support Status (in progress)

- Ongoing effort to document what parts of the engine are supported by OISF, which by community
- Currently 'tier 1', 'tier 2', community
- Tier 1: core features on most important platforms
  - E.g. AF_PACKET on Linux
- Tier 2: lesser used features and/or OS'
  - E.g. OpenBSD support

Support Status (in progress)

- Community: contributed things that have limited use cases or are just very new
- https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Support_Status

Code Quality

- Stick with our coding style (even if you don't like it)
- Documented on our redmine
- When in doubt, check with the dev team

Branch to target

- Bug fixes should target the stable branch(es)
  - Master-3.2.x
- Features should target development branch
- Dev branch is not open all the time
- We unofficially use 'merge windows', but we need to improve the communication around this

Commits

- Separate commits logically
- Don't mix too many things in a single commit
- No style fixes and other changes in a single commit
- Stick with correct formatting of commit messages (kernel style)
- Describe purpose and reason of change

Docs!

- Documentation is part of github repo
- If you change behavior, doc it!

Github & QA

Github workflow

- Iterative process:
- Make new Pull Request & close old (if any)
- Feedback

Github: pull request

- Template in place, please use that and be mindful of the formatting
- Describe your proposed changes
- Describe changes since your last PR on the same topic
- Add reference to redmine ticket
- Indicate what you need. Merge? Feedback? Testing? etc.

- [x] I have read the contributing guide line
  https://redmine.openinfosecfoundation.or
- [x] I have signed the Open Information S
  ids.org/about/contribution-agreement/
- [x] I have updated the user guide (in doc

Github: automated feedback

- Travis CI
- AppVeyor
- Tests: build, compile warnings, unittests, blacklisted functions
- On failure you should have all info to fix things on your own
- If you're a regular contributor, please enable Travis CI and AppVeyor on your own account as well (it's free)

Github: review phase

- Using Github 'review' capabilities
- Me or team member(s) reviewing the diff
- Most of the time this means no actual testing yet
- Often leads to change requests that should go into new PR (+new branch)

Github: manual QA

- Infamous 'PRscript' -> ETpro pcap/sid regression test
- More infamous "Victor's QA"
  - Lots of tests, code checkers, fuzzers, etc
- On failure we will try to share required info or test case where possible

regit commented 2 days ago   Member   + 😀   ✏️

Update of #2986

☑ I have read the contributing guide lines at
    https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Contributing
☑ I have signed the Open Information Security Foundation contribution agreement at https://suricata-
    ids.org/about/contribution-agreement/
☑ I have updated the user guide (in doc/userguide/) to reflect the changes made (if applicable)

Link to redmine ticket: https://redmine.openinfosecfoundation.org/issues/2253

Describe changes:

- Optional output values as array for all keys or selected
- Documentation update

PRScript output (if applicable):

- PR regit: https://buildbot.openinfosecfoundation.org/builders/regit/builds/347
- PR regit-pcap: https://buildbot.openinfosecfoundation.org/builders/regit-pcap/builds/131

Reviewers   ⚙️

🟦 jasonish   💬

🟦 victorjulien   ❌

👹 norg   🛡️ 🟠

Assignees   ⚙️

No one—assign yourself

Labels   ⚙️

None yet

Milestone   ⚙️

No milestone

Notifications

🔇 Unsubscribe

You're receiving notifications
because you were mentioned.

Post-Merge

Great, your code was accepted!

- Please stay involved to monitor how the change works
- Team will assign bug reports in this code to you
- Depending on feature and interaction support status would probably start at 'community'

Thank you for (listening|contributing)

SURICON
PRAGUE
2017