Contributing to Suricata

========================

We're happily taking patches and other contributions. The process is documented at https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Contributing Please have a look at this document before submitting.

Contribution Agreement

----------------------

Before accepting your pull requests we need you or your organization to sign our contribution agreement.

We do this to keep the ownership of Suricata in one hand: the Open Information Security Foundation. See https://suricata-ids.org/about/open-source/ and https://suricata-ids.org/about/contribution-agreement/

Contribution Process

--------------------

Suricata is a complex piece of software dealing with mostly untrusted input. Mishandling this input will have serious consequences:

\* in IPS mode a crash may knock a network offline;

\* in passive mode a compromise of the IDS may lead to loss of critical and confidential data;

\* missed detection may lead to undetected compromise of the network.

In other words, we think the stakes are pretty high, especially since in many common cases the IDS/IPS will be directly reachable by an attacker.

For this reason, we have developed a QA process that is quite extensive. A consequence is that contributing to Suricata can be a somewhat lengthy process.

On a high level, the steps are:

1. Travis-CI based build & unit testing. This runs automatically when a pull request is made.

2. Review by devs from the team and community

3. QA runs trigged by the team

Questions

---------

If you have questions about contributing, please contact us via https://suricata-ids.org/support/