Suricata - Documentation #1892

rule docs should include example rules

09/18/2016 02:34 AM - Victor Julien

Status: New
Priority: Normal
Assignee: Community Ticket
Category: 
Target version: TBD
Affected Versions: high
Effort: high
Difficulty: low
Label: Beginner

Description
Think it would be nice to add example rules for each rule keyword. Perhaps a minimal example and a real world one from the ETOpen set.

Related issues:
Related to Documentation #4706: Guide for rulewriting

History

#1 - 09/26/2016 03:26 AM - Peter Manev
It think it will also be a good idea to make that part of the PR process (as well) where such a PR introduces new or updates keywords. Otherwise the "how to" for new or updated keywords is not visible to the rulewriters or end users.
Easier said than done I suppose - it would be ideal if we can maybe have something like -
suricata --list-keywords-examples
where each listed keyword can have an example rule. Maybe we could reuse a good part of the unittests to help out with that ?

#2 - 10/09/2016 03:20 PM - Andreas Herz
Wouldn't be such a list quite verbose? Maybe we can first add it to the docs and relate to them with the --list-keywords-examples?

#3 - 05/30/2018 08:02 AM - Victor Julien
- Effort set to high
- Difficulty set to low

I'm open to both. I also think it would be a nice idea to have per rule keyword manpages, based on the user docs. Like how for example git commands have their own manpages. These manpages should then have one or more example rules.

#4 - 05/30/2018 08:02 AM - Victor Julien
- Assignee deleted (OISF Dev)

#5 - 05/30/2018 08:03 AM - Victor Julien
I've set effort to high as there are many keywords, but this can be a step-by-step thing. So per keyword effort is low.

#6 - 03/12/2019 11:37 AM - Victor Julien
- Assignee set to Community Ticket
- Label Beginner added

#7 - 03/12/2019 11:40 AM - Victor Julien
- Target version changed from Documentation to TBD

#8 - 09/25/2019 07:19 PM - Andreas Herz
- Tracker changed from Feature to Documentation
Related to Documentation #4706: Guide for rulewriting added