Suricata - Bug #569

display syntax requirement on keyword parsing error

09/29/2012 03:16 AM - Victor Julien

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

Description
Currently if the syntax of a rule keyword is wrong we print just a pcre error most of the times.

It would be good to have a string per keyword that is displayed on error.

Format:

threshold: type <threshold|limit|both>, track <by_src|by_dst>, count <N>, seconds <T>

History

#1 - 10/31/2012 06:38 AM - Victor Julien
- Priority changed from Normal to Low

#2 - 11/14/2012 12:08 PM - Victor Julien
- Target version changed from 1.4beta3 to 1.4rc1

#3 - 11/29/2012 05:21 AM - Victor Julien
- Target version changed from 1.4rc1 to 2.0rc2

#4 - 01/31/2014 06:48 AM - Victor Julien
- Target version changed from 2.0rc2 to 3.0RC2

#5 - 05/20/2015 06:09 AM - Victor Julien
- Target version changed from 3.0RC2 to 70

#6 - 01/29/2016 04:11 AM - Victor Julien
- Priority changed from Low to Normal
- Target version changed from 70 to TBD

#7 - 07/17/2018 08:29 AM - Victor Julien
- Assignee changed from OISF Dev to Anonymous
- Effort set to high
- Difficulty set to low

#8 - 02/23/2019 10:10 PM - Andreas Herz
- Assignee set to Community Ticket

#9 - 09/04/2019 06:22 PM - Jason Taylor
- Assignee changed from Community Ticket to Jason Taylor

#10 - 11/04/2021 12:34 AM - Jason Taylor

It looks like the last discussion that was had around this was in https://github.com/OISF/suricata/pull/4251. Are there any update thoughts or ideas

07/16/2022
around this? I was going to take another look at this but wanted to see if anyone else had or was.

#11 - 05/02/2022 12:43 PM - Jason Taylor
- Assignee changed from Jason Taylor to Community Ticket