Suricata - Feature #3199
transformation should be able to take options
09/27/2019 08:43 AM - Victor Julien

Status: Closed
Priority: Normal
Assignee: Jeff Lucovsky
Category: 
Target version: 6.0.0rc1
Effort: 
Difficulty: 

Description
Currently rule transformations cannot take options. This is due to the way it is implemented. It would be useful to allow options.

Related issues:
Blocks Feature #2290: lua: expose lua generated buffers to rule lang New
Blocks Feature #3200: pcre: allow operation as transform Closed

History
#1 - 09/27/2019 08:45 AM - Victor Julien
- Blocks Feature #2290: lua: expose lua generated buffers to rule lang added

#2 - 09/27/2019 08:50 AM - Victor Julien
- Blocks Feature #3200: pcre: allow operation as transform added

#3 - 01/20/2020 03:46 PM - Victor Julien
- Status changed from New to Assigned
- Assignee changed from OISF Dev to Jeff Lucovsky

#4 - 01/22/2020 12:25 AM - Jeff Lucovsky
This sounds like a good idea; are you suggesting it be restricted to Lua and PCRE? Or, a general purpose mechanism for these and the existing transforms?

#5 - 01/27/2020 02:06 PM - Victor Julien
I would like it to be possible to express something like

http.uri; take:4; content:"/abc";

Here 'take' would be an transform. Currently the underlying transactions code has nowhere to store this argument.

#6 - 02/18/2020 11:14 AM - Victor Julien
- Status changed from Assigned to In Review

#7 - 06/09/2020 12:09 PM - Victor Julien
- Status changed from In Review to Closed

https://github.com/OISF/suricata/pull/4919