Suricata - Feature #3626
implement from_end byte_jump keyword

04/08/2020 09:00 PM - Jason Taylor

Status: Closed
Priority: Normal
Assignee: Jeff Lucovsky
Category:
Target version: 6.0.0beta1
Effort:
Difficulty:

Description
from_end is documented:

however it is not implemented in the suricata code.

The following rule is shown as an example in the suricata docs:

```plaintext
alert tcp any any -> any any 
  (msg:"Byte_Jump From the End -8 Bytes"; 
  byte_jump:0,0, from_end, post_offset -8; 
  content:"|6c 33 33 74|"; distance:0 within:4;)
```

when attempting to load the rule the following is logged:

History
#1 - 05/12/2020 09:18 AM - Victor Julien
- Status changed from New to Assigned
- Assignee set to Jeff Lucovsky
- Target version set to 6.0.0beta1

#2 - 05/17/2020 06:47 PM - Jeff Lucovsky
- Status changed from Assigned to In Review

https://github.com/OISF/suricata/pull/4947

#3 - 07/07/2020 01:52 PM - Jeff Lucovsky
- Status changed from In Review to Closed