Suricata - Feature #2319

Expose flow lifetime to the rulelanguage

12/01/2017 05:20 AM - Stian Bergseth

<table>
<thead>
<tr>
<th>Status</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee</td>
<td>Community Ticket</td>
</tr>
<tr>
<td>Category</td>
<td></td>
</tr>
<tr>
<td>Target version</td>
<td>TBD</td>
</tr>
<tr>
<td>Effort</td>
<td></td>
</tr>
<tr>
<td>Difficulty</td>
<td></td>
</tr>
<tr>
<td>Label</td>
<td>Beginner, C, Outreachy</td>
</tr>
</tbody>
</table>

Description

During the roadmap discussion in Prague someone asked for the possibility to detect long lived sessions. VictorJ said that this data was already stored somewhere. I guess a sanity check of config for timeouts vs length of duration looked for in the signature would be a good idea

Related issues:

- Related to Task #2309: SuriCon 2017 brainstorm
- Related to Feature #3271: Add keyword to determine flow based speed/bw

History

#1 - 12/01/2017 05:26 AM - Victor Julien
- Related to Task #2309: SuriCon 2017 brainstorm added

#2 - 12/01/2017 05:26 AM - Victor Julien
- Target version set to TBD

#3 - 04/14/2018 07:25 AM - Victor Julien
Stian are you planning to submit an implementation for this?

#4 - 07/17/2018 10:11 AM - Victor Julien
- Assignee changed from Stian Bergseth to Anonymous
- Effort set to low
- Difficulty set to low

#5 - 02/23/2019 10:05 PM - Andreas Herz
- Assignee set to Community Ticket

#6 - 03/12/2019 11:59 AM - Victor Julien
- Label Beginner, Outreachy added

#7 - 10/22/2019 01:58 PM - Andreas Herz
- Related to Feature #3271: Add keyword to determine flow based speed/bw added

#8 - 11/01/2019 01:21 PM - Andreas Herz
- Assignee changed from Community Ticket to Stian Bergseth

Additional ideas we will split into dedicated issues:
- Dump the flow table over unix socket.
- Explore also loading the flow table into suricata as part of a state keeping.

#9 - 09/21/2020 02:22 PM - Victor Julien
- Assignee changed from Stian Bergseth to Community Ticket
- Effort deleted (low)
- Difficulty deleted (low)
- Label C added