Suricata - Feature #1608

Add option to disable JSON escape slash

11/30/2015 11:57 AM - Zach Rasmor

<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>low</td>
</tr>
<tr>
<td>Difficulty:</td>
<td>low</td>
</tr>
</tbody>
</table>

Description

We like to have the ability to search (grep) through JSON logs without de-serialization, however this becomes very tedious with the default presence of the JSON escape slash. I was planning to generate a patch to remove the JSON_ESCAPE_SLASH flag from the json_dump_callback function to fit our needs, however I am also happy to put in a little more effort to instead make this an option and contribute it back.

Let me know if this is something that the community would be interested in.

History

#1 - 11/30/2015 12:11 PM - Victor Julien
I wonder if this could/should be default behaviour. Not sure why we enable this option. Thoughts anyone?

#2 - 01/01/2016 05:57 PM - Andreas Herz
- Assignee set to OISF Dev
- Target version set to TBD

#3 - 05/30/2018 08:27 AM - Victor Julien
- Status changed from New to Assigned
- Assignee changed from OISF Dev to Zach Rasmor

Care to submit a patch Zach?

#4 - 07/17/2018 10:37 AM - Victor Julien
- Assignee changed from Zach Rasmor to Anonymous
- Effort set to low
- Difficulty set to low

#5 - 02/23/2019 10:17 PM - Andreas Herz
- Assignee set to Community Ticket

#6 - 06/30/2019 06:41 PM - Shivani Bhardwaj
Is this still relevant? Can I work on this?

#7 - 09/27/2019 01:38 PM - Victor Julien
- Status changed from Assigned to New