Suricata - Documentation #4671

Document changes to HTTP events with respect to http/http2 normalization

09/10/2021 03:05 PM - Jason Ish

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Jason Ish</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>7.0rc1</td>
</tr>
<tr>
<td>Affected Versions:</td>
<td></td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td></td>
</tr>
</tbody>
</table>

Description

Probably something in the upgrade section of the guide.

History

#1 - 09/10/2021 03:05 PM - Jason Ish
- Target version set to 7.0rc1

#2 - 09/15/2021 07:11 AM - Victor Julien
- Assignee set to Philippe Antoine

#3 - 09/15/2021 11:42 AM - Philippe Antoine
Jason, What is expected here?
Is this about rules/http2-events.rules?

#4 - 09/21/2021 05:35 PM - Jason Ish
Maybe I was wrong, but are the "http" events in "eve.json" changing in format at all?

#5 - 09/22/2021 12:59 PM - Philippe Antoine

Maybe I was wrong, but are the "http" events in "eve.json" changing in format at all?

They should have the same info such as http.url or http.http_method
They are extended as we have more http2-specific information
We can recognize them with http.version: "2"
You can check for instance S-V test http2-upgrade
You can check the code in log_http2 with for (name, value) in common {

#6 - 09/29/2021 11:37 AM - Philippe Antoine
- Status changed from New to Feedback
- Assignee changed from Philippe Antoine to Jason Ish

#7 - 01/17/2022 07:51 PM - Jason Ish
- Status changed from Feedback to Closed

Thanks. I think this can be closed.