Suricata - Feature #1191

EVE log does not support customformat

05/08/2014 03:24 PM - Paul Gofran

<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>medium</td>
</tr>
</tbody>
</table>

Description

HTTP logging with EVE log does not support the customformat tag. It would be beneficial to have consistent features between EVE logging and regular http-log which does support the customformat tag.

This is similar to #1150 where tls.store can not be used with EVE log.

History

#1 - 05/09/2014 07:31 AM - Victor Julien

Does this do what you need? [https://github.com/inliniac/suricata/pull/956](https://github.com/inliniac/suricata/pull/956)

It allows for extra logging of http headers, although it's limited to a hardcoded list currently: [https://github.com/inliniac/suricata/pull/956/files#diff-544ba33b2a4e8950a3c135a9717f319dR130](https://github.com/inliniac/suricata/pull/956/files#diff-544ba33b2a4e8950a3c135a9717f319dR130)

#2 - 05/09/2014 08:54 AM - Paul Gofran

A few things that we would like to see in addition to this are some of the things identified in #602:

Cookie parsing: ex "%(Foobar)C"
Max length: ex: "%(100)\[Referer]\"

Also I did not see User-Agent in this list.
If HTTP_FIELD_SIZE could be broken up into request size and response size that would also be helpful.

#3 - 05/09/2014 08:56 AM - Victor Julien

- Tracker changed from Bug to Feature

UA is printed to the log by default. On the rest: sensible requests :)

#4 - 01/01/2016 06:08 PM - Andreas Herz

- Assignee set to OISF Dev
- Target version set to TBD

#5 - 07/17/2018 08:51 AM - Victor Julien

- Assignee changed from OISF Dev to Anonymous
- Effort set to low
- Difficulty set to medium

#6 - 02/23/2019 09:55 PM - Andreas Herz

- Assignee set to Community Ticket