Suricata - Documentation #2620

Documentation: tagged_packets / event_type packet

09/14/2018 02:20 PM - Jack Mott

<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>TBD</td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
<tr>
<td>Affected Versions:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td></td>
</tr>
</tbody>
</table>

Description
Improve logging documentation around tagged_packets and eve json field "event_type packet".

Related issues:
Related to Documentation #2699: document all eve record types and fields

Assigned

History

#1 - 09/19/2018 09:08 PM - Andreas Herz
- Target version set to Documentation

We need to add it to the keywords section as well to the EVE (JSON Format) section.

Suggested example rule:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN HackerDefender? Root Kit Remote Connection Attempt Detected"; flow: established, to_server; content:"|01 9a 8c 66 af c0 4a 11 9e 3f 40 88 12 2c 3a 4a 84 65 38 b0 b4 08 0b af db ce 02 94 34 5f 22|"; rawbytes; tag: session, 20, packets; reference:url,securityresponse.symantec.com/avcenter/venc/data/backdoor.hackdefender.html; reference:url,doc.emergingthreats.net/2001743; classtype:trojan-activity; sid:2001743; rev:8; metadata:created_at 2010_07_30, updated_at 2010_07_30;)
```

#2 - 11/21/2018 02:46 PM - Victor Julien
- Related to Documentation #2699: document all eve record types and fields added

#3 - 03/11/2019 02:25 PM - Victor Julien
- Assignee set to Community Ticket

#4 - 03/12/2019 11:34 AM - Victor Julien
- Target version changed from Documentation to TBD

#5 - 09/25/2019 07:20 PM - Andreas Herz
- Tracker changed from Optimization to Documentation