Suricata - Feature #1323
automated eve.json rotation
11/25/2014 09:13 AM - god lol

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

Description
Right now .pcap files are rotated by suricata after reaching configurable limit but eve.json grows eternally unless external tool is involved. Would be nice to get rid of such inconsistency and have configuration option to rotate eve.json the same way .pcap files are rotated.

History
#1 - 11/25/2014 02:33 PM - Peter Manev
You can achieve the same with logrotate - it actually offers much more flexibility.

#2 - 11/25/2014 02:33 PM - Peter Manev
- Tracker changed from Bug to Feature

#3 - 11/25/2014 02:42 PM - god lol
Yes, that's what I use as a workaround but I really would prefer to have self-contained configuration for suricata. This way if I'm migrating from host A to host B I could move only /etc/suricata without bothering with bunch of external configs.

#4 - 01/01/2016 05:52 PM - Andreas Herz
- Assignee set to Anonymous
- Target version set to TBD

#5 - 06/12/2018 05:43 PM - Jason Ish
- Effort set to medium
- Difficulty set to medium

This comes up every so often. A common example is unified2 logging, where the size is limited, and filenames are suffixed with a timestamp.

Note that we're close. Time based rotation can be done, http://suricata.readthedocs.io/en/suricata-4.0.4/output/eve/eve-json-output.html#output-eve-rotate. Still this doesn't do any cleanup.

We should decide if cleanup should be a feature of Suricata, or if its not, by design. Then we can close out this issue and have an answer for future requests of the same nature.

#6 - 02/23/2019 10:16 PM - Andreas Herz
- Assignee set to Community Ticket

#7 - 03/11/2021 09:50 AM - Philippe Antoine
- Status changed from New to Closed

https://github.com/OISF/suricata/pull/5463

03/06/2022