Suricata - Feature #4853

eve: Add information about Suricata version

11/24/2021 10:30 AM - Juliana Fajardini Reichow

<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>Juliana Fajardini Reichow</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
</tbody>
</table>

Description

Having that information on the eve log could be useful when trying to offer support, since that file is the one folks often share, when some behavior is not as expected.

We could then skip asking that, if that info was already available.

Victor suggests that a way of achieving that would be to enable suricata.log by default and add that info to eve.json

It has also been discussed the possibility of adding a first record to the logs that would contain some of this type of info in a special record type

History

#1 - 11/26/2021 06:51 AM - Victor Julien
- Subject changed from Add information about Suricata version to eve-log to eve: Add information about Suricata version

#2 - 11/29/2021 06:59 PM - Jason Ish

Adding a record on startup would be great, and I know this topic has come up before. However, its more useful in a log aggregation system, unfortunately it won't help us with asking people to provide the version, as they're more likely to include the log records of interest, which will not be the first one. So I think the issues should be considered separately.

One option I see is adding the Suricata version to the stats log, since we often ask for that. This almost eliminates the need for a startup record. A stats record with the Suricata version and the uptime (already existing) gives us almost the same info. However I suppose a startup message could include more information like interface, mode, command line parameters of note.

Or just simply adding the Suricata version to the eve record itself...

```
{
  "timestamp": "2021-07-28T16:03:38.471697-0600",
  "version": "6.0.4",
  "flow_id": 422765781370987,
  ...
}
```

its pretty small in size compared to a full eve record.