Suricata - Feature #1369
eve: json schema
01/21/2015 05:48 AM - Victor Julien

| Status:    | Closed          |
| Priority:  | Normal          |
| Assignee:  | Jason Ish       |
| Category:  |                |
| Target version: | 7.0rc1         |
| Effort:    | Label:          |

Description
http://json-schema.org/implementations.html

We could create a schema that we then can use to validate the json output, at least in QA.

Related issues:
- Related to Feature #3975: Suricata-Verify: Add JSON schema validation to EVE ...
  New
- Related to Bug #4860: eve.json remove app-layer specific fields from root object
  Closed

History
#1 - 01/21/2015 11:17 AM - Peter Manev
  Maybe we could use IDSDB to utilize it in - https://github.com/EmergingThreats/IDSDeathBlossom

#2 - 05/20/2015 09:17 AM - Victor Julien
  - Assignee set to Anonymous

#3 - 06/12/2018 05:36 PM - Jason Ish
  - Effort set to high
  - Difficulty set to low

#4 - 02/23/2019 10:16 PM - Andreas Herz
  - Assignee set to Community Ticket

#5 - 11/30/2020 05:40 PM - Jason Ish
  - Related to Feature #3975: Suricata-Verify: Add JSON schema validation to EVE output. added

#6 - 12/24/2020 06:34 AM - Tharushi Jayasekara
  - Assignee changed from Community Ticket to Tharushi Jayasekara

#7 - 12/29/2020 05:50 AM - Tharushi Jayasekara
  - Assignee deleted (Tharushi Jayasekara)

#8 - 12/29/2020 05:50 AM - Tharushi Jayasekara
  - Assignee set to Community Ticket

#9 - 01/19/2021 04:16 PM - Tharushi Jayasekara
  - Assignee changed from Community Ticket to Tharushi Jayasekara

#10 - 02/09/2021 03:54 PM - Jason Ish
  - Status changed from New to In Review

PR: https://github.com/OISF/suricata-verify/pull/431
#11 - 11/27/2021 06:08 AM - Victor Julien
- Assignee changed from Tharushi Jayasekara to Philippe Antoine

[link to GitHub](https://github.com/OISF/suricata-verify/pull/586)

#12 - 11/30/2021 01:20 PM - Philippe Antoine
- Related to Bug #4860: eve.json remove app-layer specific fields from root object added

#13 - 04/25/2022 01:23 PM - Philippe Antoine
[link to GitHub](https://github.com/OISF/suricata-verify/pull/797)

#14 - 05/31/2022 08:39 AM - Philippe Antoine
- Assignee changed from Philippe Antoine to Jason Ish

[link to GitHub](https://github.com/OISF/suricata/pull/7412)

#15 - 06/03/2022 08:57 AM - Victor Julien
- Status changed from In Review to Closed
- Target version changed from QA to 7.0rc1
- Effort deleted (high)
- Difficulty deleted (low)

#16 - 06/03/2022 08:57 AM - Victor Julien
- Subject changed from json schema to eve: json schema