Suricata - Feature #4060
createst: Commandline param to specify minimum required version of Suricata

10/07/2020 03:38 PM - Shivani Bhardwaj

Status: In Review
Priority: Normal
Assignee: Tharushi Jayasekara
Category:
Target version: QA
Effort:
Difficulty:

Label: Beginner, Outreachy, Python

Description
Current createst script generates only the filter blocks as per eve.json, extend its functionality to add a global minimum required version of Suricata as mentioned on command line.

Expectation
createst.py mytest mypcap --add-min-version 5.0

The final generated test.yaml should have a min suricata version defined globally. e.g. https://github.com/OISF/suricata-verify/blob/master/tests/flowbit-oring/test.yaml

History
#1 - 10/07/2020 03:45 PM - Shivani Bhardwaj
- Description updated

#2 - 10/07/2020 03:52 PM - Shivani Bhardwaj
- Target version set to QA

#3 - 10/08/2020 07:19 AM - Anuradha jha
- Assignee changed from Community Ticket to Anuradha jha

#4 - 10/19/2020 09:32 AM - Anuradha jha
- Assignee changed from Anuradha jha to Community Ticket

#5 - 10/20/2020 04:49 AM - Tharushi Jayasekara
- Assignee changed from Community Ticket to Tharushi Jayasekara

#6 - 10/24/2020 04:20 AM - Tharushi Jayasekara
Shivani Bhardwaj wrote:

```
Current createst script generates only the filter blocks as per eve.json, extend its functionality to add a global minimum required version of Suricata as mentioned on command line.
```

Expectation

```
[...]
```

The final generated test.yaml should have a min suricata version defined globally. e.g. https://github.com/OISF/suricata-verify/blob/master/tests/flowbit-oring/test.yaml

Hi Shivani,

Just a small question regarding the wording of the commandline param. Could I change it to "min-version" so that the it is consistent with the existing params, or should I use "add-min-version" as given in the text?

#7 - 10/30/2020 06:19 AM - Tharushi Jayasekara
- Status changed from New to In Review

PR: [https://github.com/OISF/suricata-verify/pull/353](https://github.com/OISF/suricata-verify/pull/353)