Suricata - Feature #2644
Add direction of stream to eve-json events
10/22/2018 01:45 PM - Stian Bergseth

<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>Stian Bergseth</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>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Description:</td>
<td>Add a direction field in eve-json to indicate what direction the stream started with.</td>
</tr>
</tbody>
</table>

Related issues:
Related to Feature #2628: Specify the flow direction in metadata sent by Suri...

History

#1 - 12/10/2018 02:10 PM - Daniel Jaraud
I confirm, this would be great. It's a problem I'm frequently having trouble with. For now I'm just checking whether flow_id value has been seen before or not, but it's a rather complex and costly way of doing it. It's also causing troubles when I'm looking to graph data coming from eve.json, there's no easy way to know if the connexion is related to a former event or not.

#2 - 12/10/2018 02:12 PM - Daniel Jaraud
This feature may be related: [https://redmine.openinfosecfoundation.org/issues/2628](https://redmine.openinfosecfoundation.org/issues/2628) and I think both could be merged.

#3 - 12/12/2018 02:44 PM - Victor Julien
Some work has been done by Stian, but I think we need a bit more on the QA side to validate that the field is always correct, see: [https://github.com/OISF/suricata/pull/3521#issuecomment-446604186](https://github.com/OISF/suricata/pull/3521#issuecomment-446604186)
Help on this would be much appreciated!

#4 - 12/13/2018 08:00 PM - Daniel Jaraud
Hi Victor,
I'm going to have a serious look at it and will report on my tests.
Thanks a lot for the update.

#5 - 12/14/2018 02:59 PM - Daniel Jaraud
Hi Victor,
Got the work done by Stian patched on both 3.2 and master branch in production, as well as on brand new installs over the last day.
With libhtp installed and a ./configure --enable-hiredis --prefix=/usr/ --sysconfdir=/etc/ --localstatedir=/var/.
The field is empty only in case of app_proto failed (flow timeout) or when tcp_state is closed, which seems OK to me.
I tested the master branch with ../suricata-verify-master/run.py > results.log, here is the result:
@
===> alert-testmyids: OK
===> alert-testmyids-not-established: OK
===> dnp3: OK
===> dnp3-dnp3_data-alert: OK
===> dnp3-dnp3_func-alert: OK
===> dns-eve: OK
===> dns-eve-v2-udp-dig-a-www-suricata-ids-org: OK
===> dns-json-log: OK
===> dns-lua-rules: SKIPPED: requires feature HAVE_LUA
===> dns-single-request: OK
===> dns-tcp-multirequest-buffer-1: OK
===> dns-tcp-ts-gap: OK
===> dns-tcp-www-google-com: OK
===> dns-udp-dig-a-www-suricata-ids-org: OK
===> dns-udp-dns-log-unanswered: OK
===> dns-udp-double-request-response: OK
===> dns-udp-eve-log-aaaa-only: OK

07/15/2022
So this look fine to me, the feature gives great enhancement for my SIEM, especially for graphs and live maps, as well as for operators quick understanding of flows.

Please let me know if you need more testing.

#6 - 12/15/2018 01:37 PM - Daniel Jaraud
Feature request #2628 can be closed (fixed by this feature request).

#7 - 12/18/2018 03:47 PM - Victor Julien
Hi Daniel, what I meant was a new set of tests for suricata-verify to show that the new functionality works correctly in the various scenarios. Unless I'm missing something I don't see that in the output above, correct?

#8 - 06/15/2019 09:50 PM - Andreas Herz
- Target version set to TBD

#9 - 09/26/2019 01:35 PM - Victor Julien
- Related to Feature #2628: Specify the flow direction in metadata sent by Suricata. added