Suricata - Support #3704

Suricata alerts don't show up in Prelude-SIEM

05/18/2020 02:23 PM - Little Yu

<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>Affected Versions:</td>
<td></td>
</tr>
</tbody>
</table>

Description
Hello,

I've been trying for the past week to configure both Suricata and Prelude but it seems like Suricata alerts don't show up in Prelude even though I've added it to prelude and the alerts show up in fast.log normally.

Can you help me?

Thanks

History

#1 - 05/18/2020 07:33 PM - Victor Julien
- Tracker changed from Bug to Support
- Assignee set to Community Ticket
- Priority changed from Immediate to Normal

#2 - 05/18/2020 08:37 PM - Andreas Herz
Can you share more details about your setup/configuration?

#3 - 05/18/2020 09:30 PM - Thomas Andrejak
Hello

We need these information:

- Linux Distribution
- Version of Prelude ? With packets ?
- Version of suricata ? With packets ?
- Triggered rules that should shows up in Prelude ?

You can download a prepared iso with Prelude and Suricata included here: [https://www.prelude-siem.org/pkg/prelude_va/prelude-oss-v5.1.0.iso](https://www.prelude-siem.org/pkg/prelude_va/prelude-oss-v5.1.0.iso)

Regards

#4 - 05/19/2020 10:07 AM - Little Yu
Andreas Herz wrote in #note-2:

Can you share more details about your setup/configuration?

Hi, thanks a lot for your answer but I've finally resolved it. I don't know what the problem was as all I did was deleted everything and install it again with the same setup/config.

Thanks again!

#5 - 05/19/2020 10:15 AM - Victor Julien
- Status changed from New to Closed