Suricata - Feature #590

document pulledpork for rule updates

10/05/2012 03:08 AM - Victor Julien

<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></td>
</tr>
<tr>
<td>Category</td>
<td>Documentation</td>
</tr>
<tr>
<td>Target version</td>
<td>Documentation</td>
</tr>
<tr>
<td>Effort</td>
<td></td>
</tr>
<tr>
<td>Difficulty</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
</tbody>
</table>

we have it for oinkmaster: https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Rule_Management_with_Oinkmaster

History

#1 - 06/17/2015 08:20 AM - Andreas Moe
Thinking that maybe this falls abit outside the scope of the suricata docs? Using suricata will be the same regardless of what rulemanagement framework a person uses.

#2 - 06/17/2015 12:27 PM - Victor Julien
I think it's a critical step for most users to use a rule manager, with generally a few Suricata specific aspects. So it would make sense for us to document it, and also to recommend it to users.

#3 - 12/22/2015 04:09 PM - Andreas Herz
- Assignee set to Andreas Herz

#4 - 02/07/2016 04:43 PM - Andreas Herz
Does anyone have a working pulledpork.conf for Suricata and ETOpen?

#5 - 02/08/2016 04:41 PM - Andreas Herz
- Assignee changed from Andreas Herz to Anonymous

#6 - 07/03/2017 04:21 AM - Fanny Dwargee
Hi,

there's just one thing that Pulledpork currently lacks for Suricata and that's the signal compatibility (Snort uses SIGHUP for reloading its rules and it's harcoded into the Pulledpork code).

That GitHub PR https://github.com/shirkdog/pulledpork/pull/274 provides full support for Suricata signal compatibility but I'm afraid the Pulledpork guy it's a bit lazy accepting PR. :) 

I myself use the current version of Pulledpork with the aforementioned patch and works like a charm, so, in the end the key points are just changing (apart from the common options for the rules) the pid_path and the snort version in the pulledpork.conf file this way:

```
pid_path=/usr/local/var/run/suricata.pid
snort_version=suricata-4.0
```

Hope that helps

#7 - 07/03/2017 04:25 AM - Fanny Dwargee
Forgot to mention how run Pulledpork with the above patch:

```
pulledpork.pl -H SIGUSR2 -c /usr/local/etc/pulledpork/pulledpork.conf -E -T
```

#8 - 06/12/2018 05:48 PM - Jason Ish
- Effort set to low
- Difficulty set to low

06/13/2020
I'd like to suggest closing this ticket. I think it should be up to Pulled Pork to document using it for Suricata. I'd suggest the same for Oinkmaster, but for historical reasons maybe it should stay. However, once Suricata-Update is bundled, maybe we should remove Oinkmaster documentation as well.

#9 - 11/04/2018 09:39 AM - Victor Julien
- Status changed from New to Closed
- Effort deleted (low)
- Difficulty deleted (low)