Suricata - Feature #821
conditional logging: output steering
06/10/2013 10:18 AM - Matt Carothers

<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>Community Ticket</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
<tr>
<td>Effort:</td>
<td>medium</td>
</tr>
<tr>
<td>Difficulty:</td>
<td>high</td>
</tr>
</tbody>
</table>

**Description**

I would like to be able to log (or not) in various formats on a rule-by-rule basis. For example, I would like to see all HTTP requests directed at a particular sinkhole. It would be nice if I could simply add a rule like this:

```
alert tcp $HOME_NET any -> $SINKHOLE_NET 80 (msg:"Sinkhole HTTP"; content:"GET /"; log:http;)
```

Or better yet, I'd like to be able to define my own log keywords in suricata.yaml in order to direct debug, pcap, or http logging at different files for different rules.

```
outputs:
  - debug
    format: alert-debug
    enabled: conditional # 'yes' - enable for all alerts, 'no' - disable, 'conditional' - enable for rules using a log keyword
    filename: alert-debug1.log
    append: yes
  - sinkhole-http
    format: http-log
    enabled: conditional
    filename: sinkhole-http.log
    append: yes
```

```
alert tcp $HOME_NET any -> $SINKHOLE_NET 80 (msg:"Sinkhole HTTP"; content:"GET /"; log:sinkhole-http;)
alert tcp any 84 -> $HOME_NET any (msg:"Investigating strange traffic"; log:debug1;)
```

**Related issues:**

- Related to Feature #1005: conditional logging: controlling what gets logged

**History**

#1 - 10/26/2013 10:21 AM - Victor Julien
- Target version set to TBD

#2 - 01/01/2016 06:17 PM - Andreas Herz
- Assignee set to OISF Dev

#3 - 05/02/2017 04:19 PM - Andreas Herz
- Related to Feature #1005: conditional logging: controlling what gets logged added

#4 - 05/02/2017 04:19 PM - Andreas Herz
- Related to Feature #1005: conditional logging: controlling what gets logged added

#5 - 05/02/2017 04:20 PM - Andreas Herz
- Related to deleted (Feature #1005: conditional logging: controlling what gets logged)

#6 - 07/17/2018 08:44 AM - Victor Julien
- Assignee changed from OISF Dev to Anonymous

06/13/2020
- Effort set to medium
- Difficulty set to high

#7 - 02/23/2019 10:12 PM - Andreas Herz
- Assignee set to Community Ticket

#8 - 09/25/2019 07:32 PM - Victor Julien
What about a option to make a logger depend on the presence of a flowbit? Then rules can set this.

#9 - 11/07/2019 10:37 AM - Victor Julien
- Subject changed from Conditional logging to conditional logging: output steering