**Suricata - Feature #1469**

**Use ISO 8601 date/time formats**

05/13/2015 01:51 PM - James Moe

<table>
<thead>
<tr>
<th>Status:</th>
<th>Assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>OISF Dev</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>
</tbody>
</table>

**Description**

suricata (as of 2.0.7) uses a date format that can be confusing. The log files have the US standard form "mm/dd/yyyy". However, when looking at the output of the "-v" option, the date form is "dd/mm/yyyy", a European preference, using slashes instead of dots. The ambiguity becomes obvious only when the day of month exceeds 12.

The feature request is an option in <suricata.yaml> to select a date format between its current form and an ISO 8601 form; my preference is "2015-05-13T09:00:24".


**Related issues:**

- Related to Optimization #1718: Time stamp in Log files should be ISO 8601 format

**History**

#1 - 01/01/2016 05:47 PM - Andreas Herz
- Assignee set to OISF Dev
- Target version set to TBD

#2 - 12/21/2017 07:13 AM - Victor Julien
- Status changed from New to Assigned
- Assignee changed from OISF Dev to Richard Sailer
- Target version changed from TBD to 70

I think it would be good to add support for the ISO form in console logging as well. CreateISOStringString() can be used in SCLogMessageGetBuffer() in util-debug. The messages are constructed based on a format string which defaults to SC_LOG_DEF_LOG_FORMAT. I would suggest adding a new format specifier.

#3 - 02/18/2019 10:16 PM - Andreas Herz
- Assignee changed from Richard Sailer to OISF Dev

#4 - 05/28/2019 09:16 PM - Andreas Herz
- Related to Optimization #1718: Time stamp in Log files should be ISO 8601 format added

#5 - 08/07/2020 01:55 PM - Victor Julien
- Target version changed from 70 to TBD