### Suricata - Task #3302

**Research: ruleset optimizations**

11/01/2019 04:31 PM - Andreas Herz

<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></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
</tbody>
</table>

**Description**

The suggestion at Suricon 2019 was to have an analyzer that inspects a ruleset and compiles it into a more optimized form.

An example: if there are many similar rules for matching a DNS query, perhaps this logic could automatically convert this into a single rule + a dataset.

The purpose of this ticket is to research what those optimizations could be and test if they actually improve performance.

**Related issues:**

Related to Task #3288: Suricon 2019 brainstorm

**History**

**#1 - 11/02/2019 08:38 AM - Victor Julien**
- Description updated

**#2 - 11/02/2019 10:11 AM - Victor Julien**
- Assignee changed from OISF Dev to Community Ticket

I think it would be great if some test cases could be built, and then tested against pcaps and replay.

E.g. 1000 dns rules vs 1 dataset rule.

Perhaps we can ask Brad to use his replay setup to test the results.

**#3 - 11/05/2019 10:51 AM - Victor Julien**
- Parent task deleted (#3288)

**#4 - 11/05/2019 10:51 AM - Victor Julien**
- Related to Task #3288: Suricon 2019 brainstorm added