**Suricata - Feature #2281**

**tcp stream: simpler IDS handling of overlap evasions**

11/20/2017 09:56 AM - Victor Julien

<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>Victor Julien</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**

Currently we act only on 'ACKed' data so we can use target based reassembly to prevent evasions. This leads to 2 issues:

1. detection/logging always a bit delayed, which is worse in case of sudden flow cut offs. Then handling waits for flow timeout.
2. nobody ever sets the OS/ip mapping.

The idea of this ticket is to act on non-ACK'd data right away, and simply issue a warning (event) if data is different.

**Related issues:**

- Related to Task #2309: SuriCon 2017 brainstorm
  - New

- Related to Task #3288: Suricon 2019 brainstorm
  - New

**History**

### #1 - 12/01/2017 05:02 AM - Victor Julien

- Related to Task #2309: SuriCon 2017 brainstorm added

### #2 - 11/05/2019 03:07 PM - Victor Julien

This mode of operation would look quite a bit like the inline mode for app-layer. For detection it would be a bit more involved.

### #3 - 11/05/2019 03:07 PM - Victor Julien

- Related to Task #3288: Suricon 2019 brainstorm added