Suricata - Task #5179

stats/alert: log out to stats alerts that have been discarded from packet queue

03/07/2022 05:54 PM - Juliana Fajardini Reichow

<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>Juliana Fajardini Reichow</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>7.0rc1</td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
</tbody>
</table>

Description

If certain lower priority alerts are dropped due to a given packet having achieved packet-alert-max, make sure that that data is logged to the stats.

Related issues:

- Related to Optimization #5178: detect/alert: improve packet alert queue handling
- Copied to Task #5322: stats/alert: log out to stats alerts that have been dis...
- Copied to Task #5323: stats/alert: log out to stats alerts that have been dis...

Rejected

Closed

Closed

History

#1 - 03/07/2022 05:54 PM - Juliana Fajardini Reichow
- Related to Optimization #5178: detect/alert: improve packet alert queue handling added

#2 - 04/05/2022 07:48 PM - Juliana Fajardini Reichow
- Status changed from New to In Progress

#3 - 04/05/2022 09:17 PM - Juliana Fajardini Reichow
- Status changed from In Progress to In Review

PR for review: https://github.com/OISF/suricata/pull/7209

#4 - 05/02/2022 12:52 PM - Juliana Fajardini Reichow
- Status changed from In Review to Closed

Merged PR: https://github.com/OISF/suricata/pull/7347

#5 - 05/02/2022 11:39 PM - Juliana Fajardini Reichow
- Copied to Task #5322: stats/alert: log out to stats alerts that have been discarded from packet queue (5.0.x backport) added

#6 - 05/02/2022 11:40 PM - Juliana Fajardini Reichow
- Copied to Task #5323: stats/alert: log out to stats alerts that have been discarded from packet queue (6.0.x backport) added