Suricata - Bug #497

rule-analyzer depth/offset warnings not counted

07/06/2012 02:47 PM - Eileen Donlon

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Low</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Anoop Saldanha</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>1.3.1</td>
</tr>
<tr>
<td>Affected Versions:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td></td>
</tr>
</tbody>
</table>

Description
The depth/offset warnings do not increment the rule_warning counter, so they are not reported in the warnings-only mode for the rule-analyzer if they are the only warnings for a rule.

History
#1 - 07/07/2012 03:57 AM - Victor Julien
- Status changed from New to Assigned
- Priority changed from Normal to Low
- Target version set to 1.4beta1
- Estimated time set to 0.50 h

Warning only mode can be tested with:

```
engine-analysis:
    # enables printing reports for fast-pattern for every rule.
    rules-fast-pattern: yes

rules: warning-only
```

#2 - 07/11/2012 06:33 AM - Victor Julien
- Status changed from Assigned to Closed
- Target version changed from 1.4beta1 to 1.3.1

Fixed by patch for #495.