Suricata-Update - Feature #4579
Add option for 'strict' checking for rules downloaded using the url flag
08/10/2021 03:29 PM - Ciaran O'Hagan

<table>
<thead>
<tr>
<th>Status:</th>
<th>In Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Shivani Bhardwaj</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>1.3.0</td>
</tr>
<tr>
<td>Effort:</td>
<td>low</td>
</tr>
<tr>
<td>Difficulty:</td>
<td>low</td>
</tr>
<tr>
<td>Label:</td>
<td></td>
</tr>
</tbody>
</table>

Description
Following up from an email chain with Shivani.

This is a quick description of our use-case: we manage our own rules store, and each day we process new rules from Emerging Threats Open/Pro and deposit them into S3 and distribute keys to our servers running Suricata. During the update deployment, we generate pre-signed URLs from the S3 keys, and use those as parameters to the update application with no-merge enabled. On top of the external rules, we have a collection of custom rules written in-house that we import using the --local flag.

However, in situations where our S3 bucket is empty (or if the S3 keys do not exist), we have found that suricata-update will report an error in the logs, but continues processing and return a 0 exit code:

```
$ echo $?
0
```

We rely on the return codes during our deployments; and these silent failures have led to misleading conclusions - where our rule deployment "succeeds" but only a very limited number of rules are actually loaded. I've created a workaround on our side to avoid this, but I think it would be great if suricata-update could be extended to include a "strict" flag, which will return an error and "fail loudly" if any of the files provided by the --url flag fail.

History
#1 - 08/26/2021 06:33 PM - Jason Ish
- Target version set to 1.3.0
- Effort set to low
- Difficulty set to low

I think we could do 2 things here:
1) If a URL provided by --url fails, then we just fail. As this is provided on the command line, I think we can be more strict about it than sources with an external configuration.

or

2) Like mentioned, keep the original behaviour and a --fail command line which would be a trigger to convert any errors that might get ignored to fatal, such as a ruleset download link not working.

I'd like to reserve the word strict for possible enhancements around rule parsing as already done by Suricata.

#2 - 09/07/2021 01:31 AM - Shivani Bhardwaj
- Status changed from New to Assigned

#3 - 12/27/2021 01:35 PM - Shivani Bhardwaj
- Tracker changed from Optimization to Feature
- Status changed from Assigned to In Progress

#4 - 12/27/2021 05:41 PM - Shivani Bhardwaj
- Status changed from In Progress to In Review