Suricata - Support #3426

Do rules need to change when moving on suricata5.0 ?

12/25/2019 07:48 AM - Zhu Zhu

Status: Closed
Priority: Normal
Assignee:
Category:
Affected Versions: 5.0.0
Label: Beginner, Outreachy

Description
We are planning to move on 5.0 from 4.0.3 for some reason. The rules we use in 4.0.3 include ET rules and some customized rules, and they work well in the old version. Do ET and customized rules in 4.0.3 will also work in 5.0? We don't want to change our rules actually. If they work, that's will be good news for us.

Can someone help me out? Thanks.

History
#1 - 01/20/2020 08:16 PM - Andreas Herz
  - Status changed from New to Feedback
  - Assignee set to Zhu Zhu

Unless you have very old rules with old deprecated keywords I don't expect any issues. But the best way would be to use the official 5.0.1 release and test it. If there are any issues with the rules you would get some warnings and can work on those to be fixed.

#2 - 04/26/2020 12:20 PM - Victor Julien
  - Status changed from Feedback to Closed
  - Assignee deleted (Zhu Zhu)