

Commented rules

rules

[Nuno_Santos](#) (noob17) 1 February 28, 2022, 4:21pm

Hi,

I am using the ET-open ruleset and i noticed that some of the rules are commented inside each rule file. Why some of this rules are commented? Due to FPs? Are they no longer relevant?

Thanks.

[syoc](#) 2 March 3, 2022, 2:59pm

Hi.

Might be both FP and relevancy. I would just assume that they are commented out for a good reason.

ET Open rules are provided by Proofpoint and not the Suricata developers, you might not get a better answer on this forum.

[Jeff_Lucovsky](#) (Jeff Lucovsky) 3 March 5, 2022, 1:19pm

There are several folks from Proofpoint in the community and on this forum. Suggest changing the forum title to something more descriptive to catch their attention.

[jmtaylor90](#) (jt) 4 March 5, 2022, 11:57pm

Hi,

Commented rules can be for a number of reasons. [@syoc](#) is correct, the usual reasons are indeed for excessive false positives or the rule is just no longer relevant. Another common reason is poor performance. We (proofpoint/emerging threats) will include rules that we don't otherwise have coverage for but the rules don't perform well under QA. We include such rules, because we want to provide detection but don't want to enable it by default and cause sensors to potentially drop packets due to performance problems.

Hopefully that helps

10/29/23, 11:24 PM

Commented rules - Rules - Suricata

JT

1 Like

[Nuno_Santos](#) (noob17) 5 March 8, 2022, 11:25am

Thank you! Much more clear now