Suricata - Feature #2269
TLS: tls.version: allow negation or comparison
11/13/2017 10:16 AM - B F

Status: In Review
Priority: Normal
Assignee: Community Ticket
Category: 
Target version: 7.0rc1
Effort: low
Difficulty: low

Description
According to the documentation it is possible to match on “1.0”, “1.1”, “1.2” with tls.version (http://suricata.readthedocs.io/en/latest/rules/tls-keywords.html).

I propose to
a) allow negation for this keyword, i.e. alert on all version that are NOT 1.2 for example
or
b) allow some kind of comparison with >, <, <=, >= (with would probably need some ordered table with the versions, as the version can also be SSL.

Also (at least in the case of b)) there should be a solution to cover tls.version "UNDETERMINED"

History
#1 - 11/30/2017 07:23 AM - Andreas Herz
 - Assignee set to Anonymous
 - Target version set to TBD

#2 - 07/13/2018 06:32 PM - Victor Julien
 - Effort set to low
 - Difficulty set to low

#3 - 02/23/2019 10:06 PM - Andreas Herz
 - Assignee set to Community Ticket

#4 - 03/11/2021 12:24 PM - Philippe Antoine
 - Status changed from New to In Review

https://github.com/OISF/suricata/pull/5763

#5 - 07/01/2021 01:41 PM - Philippe Antoine
 - Target version changed from TBD to 7.0rc1