Suricata - Task #3302
Research: ruleset optimizations
11/01/2019 04:31 PM - Andreas Herz

Status: New
Priority: Normal
Assignee: Community Ticket
Category: 
Target version: TBD
Effort: 
Difficulty: 
Label: 

Description
The suggestion at Suricon 2019 was to have an analyzer that inspects a ruleset and compiles it into a more optimized form.

An example: if there are many similar rules for matching a DNS query, perhaps this logic could automatically convert this into a single rule + a dataset.

The purpose of this ticket is to research what those optimizations could be and test if they actually improve performance.

Related issues:
Related to Task #3288: Suricon 2019 brainstorm

History
#1 - 11/02/2019 08:38 AM - Victor Julien
  - Description updated

#2 - 11/02/2019 10:11 AM - Victor Julien
  - Assignee changed from OISF Dev to Community Ticket

I think it would be great if some test cases could be built, and then tested against pcaps and replay.

E.g. 1000 dns rules vs 1 dataset rule.

Perhaps we can ask Brad to use his replay setup to test the results.

#3 - 11/05/2019 10:51 AM - Victor Julien
  - Parent task deleted (#3288)

#4 - 11/05/2019 10:51 AM - Victor Julien
  - Related to Task #3288: Suricon 2019 brainstorm added