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.

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.