Suricata - Feature #1389
suppress by host

02/13/2015 07:07 AM - god lol

Status: New
Priority: Normal
Assignee: OISF Dev
Category: TBD
Target version: TBD
Effort: TBD
Difficulty: TBD

Description

The problem is that rule description does not mention "suppress" at all, while the documentation on ignoring traffic is very brief and it's unclear how one could suppress alerts for the traffic going to (or from) my.host.com

History
#1 - 03/23/2015 10:17 AM - god lol
Note: suppressing based on ip is less desirable due to dyndns host.

#2 - 04/05/2015 03:26 AM - Victor Julien
I can see how this could work for http where we could use the actual hostname to match the hostname in the request, but how would this otherwise work? Would you expect suri to do the dns lookup to get the IP of the hostname?

#3 - 04/06/2015 08:34 AM - god lol
My personal use-case is SIP where it can also be extracted directly in theory (no corresponding Suricata helper yet). Although I can see how it can be handy regardless of the protocol so having infrastructure to do dns requests and cache the results for correct time would be definitely usefull.

#4 - 06/16/2016 02:52 AM - Victor Julien
- Tracker changed from Support to Feature

#5 - 09/08/2016 02:35 PM - Andreas Herz
- Assignee set to OISF Dev
- Target version set to TBD