Suricata - Feature #821
conditional logging: output steering
06/10/2013 10:18 AM - Matt Carothers

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

Description
I would like to be able to log (or not) in various formats on a rule-by-rule basis. For example, I would like to see all HTTP requests directed at a particular sinkhole. It would be nice if I could simply add a rule like this:

alert tcp $HOME_NET any -> $SINKHOLE_NET 80 (msg:"Sinkhole HTTP"; content:"GET /"; log:http;)

Or better yet, I'd like to be able to define my own log keywords in suricata.yaml in order to direct debug, pcap, or http logging at different files for different rules.

outputs:
- debug1
  format: alert-debug
  enabled: conditional # 'yes' - enable for all alerts, 'no' - disable, 'conditional' - enable for rules using a log keyword
  filename: alert-debug1.log
  append: yes
- sinkhole-http
  format: http-log
  enabled: conditional
  filename: sinkhole-http.log
  append: yes

alert tcp $HOME_NET any -> $SINKHOLE_NET 80 (msg:"Sinkhole HTTP"; content:"GET /"; log:sinkhole-http;)
alert tcp any 84 -> $HOME_NET any (msg:"Investigating strange traffic"; log:debug1;)

Related issues:
- Related to Feature #1005: conditional logging: controlling what gets logged
- Related to Feature #4172: Split eve.json into multiple files based on alert s...

History
#1 - 10/26/2013 10:21 AM - Victor Julien
- Target version set to TBD

#2 - 01/01/2016 06:17 PM - Andreas Herz
- Assignee set to OISF Dev

#3 - 05/02/2017 04:19 PM - Andreas Herz
- Related to Feature #1005: conditional logging: controlling what gets logged added

#4 - 05/02/2017 04:19 PM - Andreas Herz
- Related to Feature #1005: conditional logging: controlling what gets logged added

#5 - 05/02/2017 04:20 PM - Andreas Herz
- Related to deleted (Feature #1005: conditional logging: controlling what gets logged)
What about an option to make a logger depend on the presence of a flowbit? Then rules can set this.

Subject changed from Conditional logging to conditional logging: output steering

Related to Feature #4172: Split eve.json into multiple files based on alert severity added