Suricata - Feature #2935
Support for multiple-logger for drop eve-log
04/18/2019 07:15 AM - Ruben Louis

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

Description
Hello according to the documentation, https://github.com/OISF/suricata/blob/d6903e70c1b653984ca95f8808755efbc6a9ece4/doc/userguide/output/eve/eve-json-output.rst#multiple-logger-instances, one cannot have multiple-logger instances for the drop eve-log. Is this something that could be implemented?

History
#1 - 04/18/2019 11:41 AM - Victor Julien
- Assignee set to Community Ticket
- Target version set to TBD

The issue is that the tracking of the flow logging `flows: all|start` is done using a flag in the flow. Since the first logger would set the flag, the 2nd would not log as the flag is already set. Working around this is not impossible but would require some thought.