Suricata - Task #2381

deprecate: 'drop' log output

12/19/2017 05:21 AM - Victor Julien

Status: Closed
Priority: Normal
Assignee: Jason Ish
Category: 
Target version: 6.0.0rc1
Effort: 
Difficulty: 

Label: 

Description
Idea is to remove the ‘drop’ log facility. It has a weird output format that mimics the linux netfilter kernel messages. ‘eve.drop’ is a much better solution.

History

#1 - 12/29/2017 05:00 PM - Andreas Herz
- Assignee set to OISF Dev
- Target version set to TBD

Although I know some that are using it I guess we can deprecate it

#2 - 02/18/2019 12:58 PM - Victor Julien
- Tracker changed from Feature to Task
- Subject changed from [discussion] deprecate: ‘drop’ log output to deprecate: ‘drop’ log output
- Status changed from Feedback to Assigned


#3 - 09/24/2019 09:43 AM - Victor Julien
- Target version changed from TBD to 6.0.0rc1

#4 - 01/20/2020 03:47 PM - Jason Ish
- Assignee changed from OISF Dev to Jason Ish

#5 - 06/02/2020 05:12 PM - Jason Ish
- Status changed from Assigned to In Review

PR: https://github.com/OISF/suricata/pull/5008

#6 - 06/03/2020 03:14 PM - Jason Ish
- Status changed from In Review to Closed

Merged: https://github.com/OISF/suricata/pull/5008