Suricata - Feature #4573

add IPS drop total to eve log output

08/03/2021 01:52 PM - Corey Thomas

Status: New
Priority: Normal
Assignee: Jeff Lucovsky
Category:
Target version:
Effort:
Difficulty:
Label:

Description

It would be useful to have the stats metric for total IPS drops in eve output. Probably similar to the alert count as part of suricata engine output. The field name should be clear that it's ips or alert drops.

e.g.

{"timestamp":"2021-08-03T13:28.965147+0000","log_level":"Info","event_type":"engine","engine":{
"message":"Alerts: 56893"}}
{"timestamp":"2021-08-03T13:28.965147+0000","log_level":"Info","event_type":"engine","engine":{
"message":"IPS_Drops: 100"}}

Related issues:

Related to Feature #4756: capture: support ips stats for all IPS capture methods

In Progress

History

#1 - 10/14/2021 01:05 PM - Victor Julien
- Related to Feature #4756: capture: support ips stats for all IPS capture methods added

03/07/2022