Suricata - Task #5180

detect/alert: make sure that signatures with `drop` action are respected, even if the alert is discarded

03/07/2022 05:59 PM - Juliana Fajardini Reichow

Status: New
Priority: Normal
Assignee: Juliana Fajardini Reichow
Category:
Target version: TBD
Effort: 
Difficulty: 
Label: 

Description
Considering that an alert could be discarded from the packet queue due to queue size limitations, we must consider how signatures with the `drop` action are still taken into account, even if the respective alert is dropped.

I guess... thought must also be given with regards to how do we indicate what is going on with said traffic, even if the alert isn't kept. Debug log? Specific stats counter?

Related issues:
Related to Optimization #5178: detect/alert: improve packet alert queue handling

History

#1 - 03/07/2022 06:00 PM - Juliana Fajardini Reichow
- Related to Optimization #5178: detect/alert: improve packet alert queue handling added

#2 - 03/07/2022 06:10 PM - Juliana Fajardini Reichow
- Subject changed from detect/alert: make sure that signature with `drop` action are respected, even if the alert is discarded to detect/alert: make sure that signatures with `drop` action are respected, even if the alert is discarded