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: In Progress
Priority: Normal
Assignee: Juliana Fajardini Reichow
Category: 
Target version: 7.0rc1
Effort: 
Difficulty: 

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

Rejected

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

#3 - 04/07/2022 05:09 PM - Juliana Fajardini Reichow
- Status changed from New to In Progress

#4 - 04/11/2022 05:39 PM - Juliana Fajardini Reichow
- Status changed from In Progress to Assigned

Will stop current work on this issue because we will try to follow the approach for #4943.

#5 - 04/11/2022 05:39 PM - Juliana Fajardini Reichow
- Target version changed from TBD to 7.0rc1

#6 - 05/13/2022 12:49 PM - Juliana Fajardini Reichow
- Status changed from Assigned to In Progress

#7 - 06/02/2022 05:38 PM - Juliana Fajardini Reichow
Back to working on this.

Draft PR for appreciation and improvements: https://github.com/OISF/suricata/pull/7469