Bug # 4941 (Resolved): alerts: 5.0.8/6.0.4 count noalert sigs towards built-in alert limit

Use configurable or more dynamic @ PACKET_ALERT_MAX@

12/08/2020 12:12 PM - Philippe Antoine

Status: Closed
Priority: Normal
Assignee: Juliana Fajardini Reichow
Category: 
Target version: 7.0rc1
Effort: 
Difficulty: 
Label: 

Description
Currently, PACKET_ALERT_MAX is hardcoded to 15

This turned out to be a problem writing S-V test, with many signatures (different variations of a feature) matching on the same packet
That was HTTP keywords on HTTP2 traffic, where I had one packet containing 3 requests

It would be nice to have this value be configurable from suricata.yaml

Subtasks:
Optimization # 5178: detect/alert: improve packet alert queue handling

Related issues:
Copied to Optimization #5121: Use configurable or more dynamic @ PACKET_ALERT_MAX@ (5.0.x backport) added
Closed

#1 - 12/10/2020 02:50 PM - Victor Julien
- Assignee set to OISF Dev
- Target version changed from TBD to 7.0rc1

#2 - 05/10/2021 10:57 AM - Victor Julien
- Assignee changed from OISF Dev to Juliana Fajardini Reichow

#3 - 05/20/2021 04:36 PM - Juliana Fajardini Reichow
- Status changed from New to In Progress

#4 - 01/07/2022 09:24 AM - Victor Julien
- Priority changed from Normal to High
- Parent task set to #4941

#5 - 01/28/2022 11:07 PM - Juliana Fajardini Reichow
- Status changed from In Progress to In Review

PR for review: https://github.com/OISF/suricata/pull/6895

#6 - 02/18/2022 01:55 PM - Jeff Lucovsky
- Copied to Optimization #5121: Use configurable or more dynamic @ PACKET_ALERT_MAX@ (5.0.x backport) added

#7 - 02/18/2022 01:56 PM - Jeff Lucovsky
- Copied to Optimization #5125: Use configurable or more dynamic @ PACKET_ALERT_MAX@ (6.0.x backport) added

#8 - 05/02/2022 12:50 PM - Juliana Fajardini Reichow
Merged PR: https://github.com/OISF/suricata/pull/7347#
Status changed from In Review to Closed