Suricata - Feature #2416

Increase XFF coverage to files and http log

01/15/2018 09:00 AM - Maurizio Abba

Status: Closed
Priority: Normal
Assignee: Maurizio Abba
Category:
Target version: 4.1rc1
Effort:

Description

XFF support is restricted to alert events. It would be nice to increase its coverage to HTTP and alert.

This modification will require the transformation of the HttpXFFGetIP to accept flows instead of packets. This function will anyway only use p->flow, using the flow directly instead of the single packet will obtain the same effect and allow to get the correct IPs.

History

#1 - 01/15/2018 10:09 AM - Maurizio Abba
I'm not sure what logging would you include in this patch. Currently, XFF can be configured for eve-log and unified log. I added XFF support for files and http in eve-log. I didn't modify http.log, fast.log and metafiles.

#2 - 01/20/2018 06:15 PM - Andreas Herz
- Target version set to TBD

https://github.com/OISF/suricata/pull/3159

#3 - 07/25/2018 03:01 PM - Maurizio Abba
- Status changed from Assigned to Closed

#4 - 07/25/2018 05:33 PM - Victor Julien
- Target version changed from TBD to 4.1rc1