Suricata - Feature #4062
createst: Allow to exclude certain fields
10/07/2020 03:51 PM - Shivani Bhardwaj

Status: In Review
Priority: Normal
Assignee: Tharushi Jayasekara
Category:
Target version: QA
Effort:
Difficulty:
Label: Outreachy, Python

Description
Certain fields from the filter blocks should be allowed to be skipped.

Expectation

createst.py mytest mypcap --exclude-fields dest_port,src_port

The final generated test.yaml should have filter blocks without these fields.

Example

Before

requires:
  min-version: 5.0.0
features:
  - HAVE_LIBJANSSON

args:
  - -k none

checks:
  - filter:
      count: 1
      match:
        alert:
          action: allowed
          category: access to a potentially vulnerable web application
          gid: 1
          rev: 1
          severity: 2
          signature: nol
          signature_id: 9000000
          app_proto: http
          dest_ip: 10.100.0.8
          dest_port: 44270
          event_type: alert
          http:
            hostname: www.abcdefghij.com
            http_content_type: text/html
            http_method: GET
            http_refer: http://www.abcdefghij.com/abdeltat/login
            http_user_agent: Mozilla/5.0 (X11; U; Linux i686; fr; rv:1.9.0.6) Gecko/2009011912 Firefox/3.0.6
            length: 1483
            protocol: HTTP/1.1
            status: 401
            url: /publication/pub.home/home.html
            pcap_cnt: 14
            proto: TCP
src_ip: 162.2.41.200
csrc_port: 80

After

requires:
  min-version: 5.0.0
features:
  - HAVE_LIBJANSSON

args:
- -k none

checks:
- filter:
  count: 1
  match:
    alert:
      action: allowed
      category: access to a potentially vulnerable web application
gid: 1
rev: 1
severity: 2
signature: no1
signature_id: 9000000
app_proto: http
dest_ip: 10.100.0.8
event_type: alert
http:
  hostname: www.abcddefghij.com
  http_content_type: text/html
  http_method: GET
  http_refer: http://www.abcddefghij.com/abdeltat/login
  http_user_agent: Mozilla/5.0 (X11; U; Linux i686; fr; rv:1.9.0.6) Gecko/2009011912
                   Firefox/3.0.6
  length: 1483
  protocol: HTTP/1.1
  status: 401
  url: /publication/pub.home/home.html
pcap_cnt: 14
proto: TCP
src_ip: 162.2.41.200

History
#1 - 10/07/2020 03:52 PM - Shivani Bhardwaj
  - Target version set to QA

#2 - 10/09/2020 06:47 PM - Shreya Gupta
  @shivani, I am not able to assign this ticket to myself. I can't see any option to change the assignee. Can you please help me out?

#3 - 10/10/2020 09:16 AM - Shivani Bhardwaj
  Shreya Gupta wrote in #note-2:

  @shivani, I am not able to assign this ticket to myself. I can't see any option to change the assignee. Can you please help me out?

Could you please try again. Please log out and log in.

#4 - 10/17/2020 06:21 AM - Tharushi Jayasekara
  - Assignee changed from Community Ticket to Tharushi Jayasekara

#5 - 10/22/2020 01:24 PM - Tharushi Jayasekara
  - Status changed from New to In Review