Suricata - Feature #5262
run.py: should tell which fields are mismatching
04/11/2022 03:47 PM - Shivani Bhardwaj

Status: Assigned
Priority: Normal
Assignee: Shivani Bhardwaj
Category: 
Target version: QA
Effort: 
Label: Python

Description

Something like

Sub task 1

----------

email.to[0]: <recipient@example.com>

event_type: smtp

pcap_cnt: 89 <---- Mismatch

proto: TCP

smtp.helo: client-1016363.example.int

tax_id: 0

would be nice since it'll help us see which fields exactly to look at unless the entire event is missing.

Idea proposed by: Victor Julien

History

#1 - 04/11/2022 03:49 PM - Shivani Bhardwaj
- Description updated

#2 - 06/26/2022 08:18 PM - Victor Julien
- Assignee changed from Community Ticket to Shivani Bhardwaj