As we all know that eve.json can be outputed as json to redis. Then logstash can be used to pull the structured data from redis to elasticsearch. And I still need to store the fast.log to elasticsearch. How can I structuring fast.log and output the structed data to elasticsearch?

History

#1 - 11/02/2018 06:55 AM - Victor Julien
out of curiosity: why would you want this? The eve.alert records are trivial to pass to ES, with fast.log you will need to some kind of parsing before passing it to ES somehow

#2 - 11/05/2018 01:56 AM - Hao Han
Victor Julien wrote:

out of curiosity: why would you want this? The eve.alert records are trivial to pass to ES, with fast.log you will need to some kind of parsing before passing it to ES somehow

Thanks your replies. We want to visualize suricata's alerts with kibana.

#3 - 12/07/2018 06:20 AM - Victor Julien
I not sure I understand why you wouldn't just use the EVE alert records for this.

#4 - 02/27/2019 04:26 PM - Bryant Smith
If you are still looking for a solution here, splitting out the alert might be helpful. the eve.json will be much easier to implement in an ELK stack and this way you can send it only the alerts if that is what you are looking for.


outputs:
- eve-log:
  enabled: yes
type: file
filename: eve-ips.json
types:
  - alert
  - drop

#5 - 03/11/2019 02:17 PM - Victor Julien
- Status changed from New to Closed