It would be nice if the suricata.yaml.in file -- and hence the default configuration file -- contained at least a commented out version of
the detailed alert metadata configuration, i.e. the

```
- alert:
  #payload: yes             # enable dumping payload in Base64
  #payload-buffer-size: 4kb # max size of payload buffer to output in eve-log
  #payload-printable: yes  # enable dumping payload in printable (lossy) format
  #packet: yes             # enable dumping of packet (without stream segments)
  #http-body: yes          # Requires metadata; enable dumping of http body in Base64
  #http-body-printable: yes# Requires metadata; enable dumping of http body in printable format

  # metadata:
  # Include the decoded application layer (ie. http, dns)
  #app-layer: true

  # Log the the current state of the flow record.
  #flow: true

  #rule:
  # Log the metadata field from the rule in a structured
  # format.
  #metadata: true

  # Log the raw rule text.
  #raw: false
```

The ReadtheDocs documentation shows it ([https://suricata.readthedocs.io/en/latest/output/eve/eve-json-output.html#alerts](https://suricata.readthedocs.io/en/latest/output/eve/eve-json-output.html#alerts)) but the suricata.yaml.in only shows the metadata: yes/no switch ([https://github.com/OISF/suricata/blob/master/suricata.yaml.in#L152](https://github.com/OISF/suricata/blob/master/suricata.yaml.in#L152)). For someone who uses the example file and its comments as option documentation (such as me) that's a bit inconvenient.
Only having a subset of the possible configuration items in there would hide good functionality from users. Just my 2 cents :)  

Yeah, it's an active area of discussion. A complete suricata.yaml is pretty daunting for new users, given most of it doesn't need to be touched. I think Andreas is actively looking into better ways here.

#5 - 06/08/2020 07:04 PM - Andreas Herz

I would go with the doc link as a first quick win and include the other issue within the whole discussion. We still struggle to find the best solution to that.