http-body and http-body-printable in eve-log require metadata to be enabled, yet there is no indication of this anywhere

10/11/2018 07:24 PM - Eric Urban

| Status: | Closed |
| Priority: | Normal |
| Assignee: | Jeff Lucovsky |
| Category: | |
| Target version: | 5.0.0 |
| Affected Versions: | |
| Difficulty: | low |
| Effort: | low |

**Description**

**Summary**

In Suricata when enabling outputs.eve-log.types.alert.http-body or .http-body-printable, it is required that either outputs.eve-log.types.alert.metadata or outputs.eve-log.types.alert.http be enabled. Otherwise there is no output in the eve-log.

If this is intentional to require metadata be enabled, then it should at least be documented in the standard documentation and/or in suricata.yaml next to the config option. Another suggestion would be to have this embedded under outputs.eve-log.types.alert.metadata or .http if metadata is required in order for body logging to occur.

**Steps to reproduce**

1. Start with the default suricata.yaml config file.
2. Set outputs.eve-log.types.alert.metadata to no.
4. Generate HTTP traffic that will cause some alert to trigger.

**Actual results**

There is no http-body/http-body-response data in the eve-log. If this is by design, I was not able to find documentation supporting it.

**Expected results**

This behavior should at a minimum be documented. It would be more self-documented if the config option was nested under the metadata config option.

**History**

#1 - 10/11/2018 07:35 PM - Eric Urban

The current default config from suricata.yaml makes this confusing since the other options indented to the same level as http-body are not dependent on another config option at that same level in order to be enabled. For example, payload will be logged regardless of whether or not packet or metadata are enabled.

```yaml
- 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          # enable dumping of http body in Base64
  # http-body-printable: yes# enable dumping of http body in printable format
  metadata: yes             # add L7/applayer fields, flowbit and other vars to the alert
```

#2 - 03/11/2019 02:23 PM - Victor Julien

- Assignee set to OISF Dev

#3 - 06/15/2019 09:50 PM - Andreas Herz

- Target version set to TBD

#4 - 07/09/2019 07:23 PM - Andreas Herz

- Status changed from New to Assigned
I agree that this might be confusing, we will think about a better way of documenting that.

#5 - 09/27/2019 06:30 PM - Victor Julien
- Assignee changed from OISF Dev to Jeff Lucovsky
- Priority changed from Low to Normal
- Target version changed from TBD to 5.0.0

#6 - 09/28/2019 04:08 PM - Jeff Lucovsky
- Effort set to low
- Difficulty set to low

#7 - 10/11/2019 08:10 AM - Victor Julien
- Status changed from Assigned to Closed

https://github.com/OISF/suricata/pull/4276

#8 - 10/13/2019 08:24 AM - Victor Julien
- Tracker changed from Support to Optimization
- Affected Versions deleted (4.0.5)

#9 - 10/13/2019 08:24 AM - Victor Julien
- Tracker changed from Optimization to Documentation