Suricata - Task #4919
Add option to change sensor-name log field

12/20/2021 05:41 PM - Jason Ish

Status: New
Priority: Normal
Assignee: 
Category: 
Target version: 7.0rc1
Effort: 
Label: 
Difficulty: 

Description
Currently if the sensor-name option is set, it will be logged to eve at the top level host.

This causes an issue with Filebeat which is often used to process logs. In particular this causes an issue if not using the Filebeat Suricata module that maps Suricata events to ECS.

What Filebeat will do is overwrite the host field with its own host object, losing the Suricata sensor name. Note that if using the Suricata module the host field is retained, but remapped to suricata.eve.host, so the problem isn't so bad.

Due to the popularity of Filebeat it would be nice to change the default field name used here. Something like sensor or sensor_name would be better for tools like Filebeat, but is just generally a better name for what this field is.

I'm not sure how to handle the upgrade path. Ideally newly generated configuration files would default to this new name just as the default.

History
#1 - 12/20/2021 05:45 PM - Jason Ish

Personally I'd like this field to default to sensor_name, with an option to rename it.