Suricata - Feature #1007

united output

10/23/2013 05:22 AM - Victor Julien

Status:	Closed		
Priority:	Normal		
Assignee:	Tom DeCanio		
Category:			
Target version:	2.0rc1		
Effort:		**Label:**	
Difficulty:			

Description

Unified output for all events and alerts into a single "stream", where the stream can be a file, socket, etc.

Subtasks:

Feature # 772: JSON output for alerts	**Closed**
Feature # 542: TLS JSON output	**Closed**

History

#1 - 10/23/2013 05:30 AM - Eric Leblond

The logging format can be JSON. It should contains all the information available and be extensible:

- Output all key values possible
  - base64 encode binary
  - examples
    - all http keywords
    - stream chunk
    - packet
  - Extensibility
    - rule can set key:value
    - luajit export value
    - output matched string in alert
      - optional
      - only if significative value

#2 - 10/25/2013 04:08 AM - Victor Julien

- Status changed from New to Assigned

- Assignee set to Tom DeCanio

- Target version set to 2.0rc2

#3 - 10/25/2013 05:57 AM - Eric Leblond

- File enhanced-alerting.rst added

Attached file is proposal.

#4 - 11/14/2013 11:55 AM - Victor Julien

- Target version changed from 2.0rc2 to 2.0beta2

#5 - 12/12/2013 10:26 AM - Victor Julien

- Target version changed from 2.0beta2 to 2.0rc1

#6 - 01/31/2014 02:14 AM - Victor Julien

- Status changed from Assigned to Closed

Merged through https://github.com/inliniac/suricata/pull/807

Files