Add "status" mode to Suricata's socket command interface

03/25/2022 06:58 PM - Jeff Lucovsky

---

**Status:** New  
**Priority:** Normal  
**Assignee:** Community Ticket  
**Category:**  
**Target version:** TBD  
**Effort:**  
**Difficulty:**  
**Label:**  

**Description**
Add a status command to Suricata's socket interface that
- Is always available (when appropriate) even if Suricata is performing the initial rule load
- Returns brief status information including Suricata's "stage"

Example showing how this might look:

```python
>>> status
Success: 
"Suricata loading rules"

>>> status
Success: 
"Suricata running"
```

Additional information could be provided such as uptime, and the running and capture mode:

```python
>>> status
Success: 
"Suricata loading rules"

>>> status
Success: 
"Suricata running, 433, AF_PACKET_DEV, workers"
```

Having an always available status command means that Suricata will start the US thread earlier in its startup. This will allow enterprise monitoring to retrieve Suricata's status always, instead of only after initial rule loading and eliminates a "blackout period" during initial rule load.

---

**History**

#1 - 03/30/2022 10:42 AM - Victor Julien
- Assignee changed from OISF Dev to Community Ticket
- Target version changed from 7.0rc1 to TBD