Suricata - Feature #3084

SIP parser, logging and detection

07/11/2019 12:05 PM - Giuseppe Longo

Status: Closed
Priority: Normal
Assignee: Giuseppe Longo
Category:
Target version: 5.0rc1
Effort:
Difficulty:
Label:

Description
I'm writing a rust parser for SIP protocol, a basic logging module and adding some new keywords, see below:

- sip.method
- sip.uri
- sip.protocol
- sip.stat_code
- sip.stat_msg
- sip.request_line
- sip.response_line

Related issues:
Related to Feature #4500: RTP parser, logging and detection New

History

#1 - 07/19/2019 09:33 PM - Andreas Herz
- Status changed from New to Assigned
- Target version set to TBD

#2 - 09/18/2019 06:57 PM - Jason Ish
- Status changed from Assigned to Closed
- Target version changed from TBD to 5.0rc1

Merged to master.

Pull request: https://github.com/OISF/suricata/pull/4205

Commit:
2e975a0461ed93428a2956466688a89f61188f8d

#3 - 05/21/2021 03:22 PM - Victor Julien
- Related to Feature #4500: RTP parser, logging and detection added