Suricata - Feature #4249
SS7 Protocol Support
01/04/2021 04:20 PM - Simon Dugas

Status: Assigned
Priority: Normal
Assignee: Simon Dugas
Category: 
Target version: TBD
Effort: medium
Difficulty: medium
Label: Protocol

Description
Add support for TCAP/MAP Signalling System 7 (SS7) protocols transported on the SIGTRAN stack:

IP / SCTP / MTP2 / MTP3 / SCCP / TCAP / MAP

This includes EVE logging and detection keywords.

Addressing schemes in this stack:
- IP address & SCTP port may not be useful for signatures
- Add support for Point Code (MTP3) & Subsystem Number (SCCP)
- Add support for Global Title (SCCP)

Fields useful as detection keywords:
- Message Type (TCAP)
- Operation Code (MAP)
- Other arguments specific to op codes (MAP)

Keep in mind the various protocol standards, ANSI MAP is different from GSM MAP (ITU).

Resources
- All: ITU-T Q.700–Q.849 Series for SS7
- TCAP: ITU-T Q.771-Q.775 or ANSI T1.114
- MAP: 3GPP TS 29.002 or 3GPP2 X.S0004

Related issues:
- Related to Task #4251: SCTP support

History
#1 - 01/04/2021 05:56 PM - Victor Julien
- Status changed from New to Assigned
- Label Protocol added

Suricata's SCTP support is currently rather minimal. Is that enough for your use case or are you also planning improvements to SCTP?

#2 - 01/04/2021 06:35 PM - Simon Dugas
We are planning to extend support and at the least at session tracking.

#3 - 01/04/2021 08:32 PM - Victor Julien
- Related to Task #4251: SCTP support added