Suricata - Task #2685

Task # 4763 (Assigned): tracking: Suricon brainstorms

SuriCon 2018 brainstorm
11/15/2018 02:59 PM - Victor Julien

<table>
<thead>
<tr>
<th>Status:</th>
<th>Assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Victor Julien</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td></td>
</tr>
</tbody>
</table>

Description
Meta ticket. Add relations to this ticket for the tickets discussed at SuriCon or created after SuriCon brainstorm.

2017 edition: #2309

Related issues:
- Related to Feature #2684: Add JA3S
  Closed
- Related to Feature #2563: Add dump of all headers in http eve-log
  Closed
- Related to Task #2693: tracking: libsuricata
  In Progress
- Related to Feature #2561: Add possibility for smtp raw extraction
  Closed
- Related to Feature #2409: Push signatures without reloading the entire set.
  Rejected
- Related to Feature #2694: thresholding: feature parity between global and per...
  Closed
- Related to Feature #2695: websocket support
  Assigned
- Related to Feature #2689: http: Normalized HTTP client body buffer
  Closed
- Related to Feature #2696: http parser in rust
  In Review
- Related to Feature #2486: prefilter/fast_pattern logic for flowbits
  In Progress
- Related to Feature #2697: prefilter support for stream_size
  Closed
- Related to Feature #2698: hassh and hasshServer for ssh fingerprinting
  Closed
- Related to Feature #2282: event log aka weird.log
  Closed
- Related to Task #2278: tracking: failing better
  New
- Related to Documentation #2699: document all eve record types and fields
  Assigned
- Related to Feature #2700: ja3/ja3s functionality for IKEv2
  Assigned
- Related to Feature #2701: flow: counter for allocations at runtime
  Assigned
- Related to Feature #385: Configuration option to log all known (pcap) data fo...
  Closed
- Related to Feature #2318: matching on large amounts of data with dynamic updates
  Closed
- Related to Task #2313: tracking: save & restore state when suricata restarts
  New
- Related to Feature #2308: threshold/suppress by http_host
  Assigned
- Related to Feature #2283: turn content modifiers into 'sticky buffers'
  Closed
- Related to Feature #2713: protocol detection w/o protocol parsing
  Feedback
- Related to Feature #2754: JA3 and JA3S - sets / reputation
  Closed
- Related to Feature #2755: vendor id / vid keyword to give rulesets unique sid...
  New
- Related to Feature #2756: rules: input in json format
  New
- Related to Feature #2757: improve protocol detection
  In Review
- Related to Feature #2758: intel / reputation matching on arbitrary data
  Closed
- Related to Feature #2759: iprep: more granularity
  New

History
#1 - 11/16/2018 02:35 PM - Victor Julien
- Related to Feature #2684: Add JA3S added

09/03/2022
#2 - 11/21/2018 09:12 AM - Victor Julien  
- Related to Feature #2563: Add dump of all headers in http eve-log added

#3 - 11/21/2018 09:20 AM - Victor Julien  
- Related to Task #2693: tracking: libsuricata added

#4 - 11/21/2018 09:23 AM - Victor Julien  
- Related to Feature #2561: Add possibility for smtp raw extraction added

#5 - 11/21/2018 11:01 AM - Victor Julien  
- Related to Feature #2409: Push signatures without reloading the entire set. added

#6 - 11/21/2018 11:06 AM - Victor Julien  
- Related to Feature #2694: thresholding: feature parity between global and per-rule options added

#7 - 11/21/2018 11:16 AM - Victor Julien  
- Related to Feature #2695: websocket support added

#8 - 11/21/2018 11:28 AM - Victor Julien  
- Related to Feature #2689: http: Normalized HTTP client body buffer added

#9 - 11/21/2018 11:30 AM - Victor Julien  
- Related to Feature #2696: http parser in rust added

#10 - 11/21/2018 11:39 AM - Victor Julien  
- Related to Feature #2486: prefilter/fast_pattern logic for flowbits added

#11 - 11/21/2018 11:44 AM - Victor Julien  
- Related to Feature #2697: prefilter support for stream_size added

#12 - 11/21/2018 11:50 AM - Victor Julien  
- Related to Feature #2698: hassh and hasshServer for ssh fingerprinting added

#13 - 11/21/2018 02:41 PM - Victor Julien  
- Related to Feature #2282: event log aka weird.log added

#14 - 11/21/2018 02:41 PM - Victor Julien  
- Related to Task #2278: tracking: failing better added

#15 - 11/21/2018 02:46 PM - Victor Julien  
- Related to Documentation #2699: document all eve record types and fields added

#16 - 11/21/2018 03:14 PM - Victor Julien  
- Related to Feature #2700: ja3/ja3s functionality for IKEv2 added

#17 - 11/21/2018 03:59 PM - Victor Julien  
- Related to Feature #2701: flow: counter for allocations at runtime added

#18 - 11/24/2018 07:44 AM - Victor Julien  
- Related to Feature #385: Configuration option to log all known (pcap) data for a stream when an alert fires added

#19 - 11/24/2018 07:45 AM - Victor Julien  
- Related to Feature #2318: matching on large amounts of data with dynamic updates added

#20 - 11/24/2018 07:47 AM - Victor Julien  
- Related to Task #2313: tracking: save & restore state when suricata restarts added

09/03/2022
#21 - 11/24/2018 07:48 AM - Victor Julien
- Related to Feature #2308: threshold/suppress by http_host added

#22 - 11/24/2018 09:48 AM - Victor Julien
- Related to Feature #2283: turn content modifiers into 'sticky buffers' added

#23 - 11/24/2018 10:20 AM - Victor Julien
- Related to Feature #2713: protocol detection w/o protocol parsing added

#24 - 12/21/2018 11:29 AM - Victor Julien
- Related to Feature #2754: JA3 and JA3S - sets / reputation added

#25 - 12/21/2018 11:36 AM - Victor Julien
- Related to Feature #2755: vendor id / vid keyword to give rulesets unique sid ranges added

#26 - 12/21/2018 11:49 AM - Victor Julien
- Related to Feature #2756: rules: input in json format added

#27 - 12/21/2018 12:07 PM - Victor Julien
- Related to Feature #2757: improve protocol detection added

#28 - 12/21/2018 12:46 PM - Victor Julien
- Related to Feature #2758: intel / reputation matching on arbitrary data added

#29 - 12/21/2018 12:50 PM - Victor Julien
- Related to Feature #2759: iprep: more granularity added

#30 - 06/15/2019 09:51 PM - Andreas Herz
- Target version set to TBD

#31 - 04/26/2020 11:24 AM - Victor Julien
- Tracker changed from Support to Task
- Target version set to TBD

#32 - 10/18/2021 06:20 PM - Victor Julien
- Parent task set to #4763

#33 - 06/10/2022 11:34 AM - Victor Julien
- Status changed from New to Assigned