Suricata - Feature #535

new keywords - time, day

08/27/2012 05:02 PM - Peter Manev

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Community Ticket</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
<tr>
<td>Effort:</td>
<td>low</td>
</tr>
<tr>
<td>Difficulty:</td>
<td>low</td>
</tr>
</tbody>
</table>

Label: 

Description

It would be beneficial if we introduce "time" and "day" keywords.

ex:

alert ip any any-> any any (msg:"Time and Day based alert "; content:"login failed"; time:12.23,>,15.30; day:Saturday,Sunday;)
alert if this is between 12:23 and 15:30 on a Sunday or Saturday

the same idea here:

alert ip any any-> any any (msg:"Time and Day based alert "; content:"login failed"; day:Saturday,Sunday;)
alert ip any any-> any any (msg:"Time and Day based alert "; content:"login failed"; time:12.23,>,15.30; )

also very important:

alert ip any any-> any any (msg:"Time and Day based alert "; content:"login failed"; time:12.23,>,15.30,packet; day:Saturday,Sunday;)
where time:12.23,>,15.30,packet; is the time of the packet

and

alert ip any any-> any any (msg:"Time and Day based alert "; content:"login failed"; time:12.23,>,15.30,OS; day:Saturday,Sunday;)
where time:12.23,>,15.30,OS; is the current time of the OS

pros?

cons?

History

#1 - 08/27/2012 05:04 PM - Eric Leblond
Just thinking to that: Need to be able to treat the timezone with respect to source or destination IP ...

#2 - 08/28/2012 03:37 AM - Victor Julien
- Target version set to TBD

#3 - 01/01/2016 06:14 PM - Andreas Herz
- Assignee set to OISF Dev

#4 - 05/02/2017 04:01 PM - Andreas Herz
Wouldn't it be enough (since it's a corner case) to just use UTC?

#5 - 07/17/2018 08:27 AM - Victor Julien
- Assignee changed from OISF Dev to Anonymous
- Effort set to low
- Difficulty set to low

#6 - 02/23/2019 10:09 PM - Andreas Herz
- Assignee set to Community Ticket
Is this still valid? Can I work on this?