Suricata - Feature #425

Inspect the effects of mixing threshold and detection filters etc..

03/19/2012 07:23 AM - Anoop Saldanha

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

Description

History

#1 - 07/04/2012 04:00 AM - Victor Julien
- Target version set to 1.4

#2 - 08/29/2012 02:00 AM - Victor Julien
- Target version changed from 1.4 to 1.4beta2

Currently we ignore threshold.conf entries if a rule already has thresholding set.

As the thresholds in a rule are a list, we could just start with allowing multiple entries. The matching engine should only return a match when all conditions are met. Conflicting conditions should be checked for then obviously.

#3 - 09/24/2012 08:19 AM - Victor Julien
- Tracker changed from Bug to Feature
- Status changed from New to Assigned
- Assignee changed from Anoop Saldanha to Victor Julien

Related to #455.

#4 - 09/24/2012 08:29 AM - Victor Julien

A signature with a threshold, e.g.:

```
alert tcp any any -> any 25 (msg:"ET POLICY Inbound Frequent Emails - Possible Spambot Inbound"; flow:established; content:"mail from|3a|"; nocase; threshold: type threshold, track by_src, count 10, seconds 60; reference :url,doc.emergingthreats.net/2002087; classtype:misc-activity; sid:2002087; rev:10;)
```

Can be mixed with all types of global suppressions it seems. Tried:

```
suppress gen_id 1, sig_id 2002087, track by_src, ip xx
suppress gen_id 0, sig_id 0, track by_src, ip xx
suppress gen_id 1, sig_id 0, track by_src, ip xx
suppress gen_id 1, sig_id 2002087
```

#5 - 09/24/2012 08:37 AM - Victor Julien

```
event_filter gen_id 1, sig_id 2002087, type limit, track by_src, count 1, seconds 3600
```

Should result in 1 alert, but gets 0.

#6 - 09/24/2012 09:55 AM - Victor Julien

I've added support for suppressing thresholded sigs, but the other globals from threshold.config are not yet supported for sigs with a threshold.
#7 - 09/26/2012 02:53 AM - Victor Julien

Added support for overriding per signature thresholds.

commit 82fc61770bd3cdeb5c033bfa8f7dc2580ebf8bc
Author: Victor Julien <victor@inliniac.net>
Date: Wed Sep 26 08:58:05 2012 +0200

threshold: allow threshold.config to override rule

Allow threshold.conf to override rule thresholds in the following cases:

- threshold.config rule uses threshold or event_filter AND
- threshold.config rule applies to a single signature (so no gid 0 or sid 0)

Confirmed to work with both threshold and detection_filter rule keywords.

Part of bug #425.

#8 - 09/29/2012 03:07 AM - Victor Julien
- Target version changed from 1.4beta2 to 1.4beta3

#9 - 11/14/2012 12:08 PM - Victor Julien
- Target version changed from 1.4beta3 to 1.4rc1

#10 - 11/29/2012 05:22 AM - Victor Julien
- Target version changed from 1.4rc1 to 2.0rc2
- % Done changed from 0 to 40

Partly fixed for 1.4, work continues in 1.5.

#11 - 10/25/2013 05:51 AM - Victor Julien
- Priority changed from Normal to Low

#12 - 01/31/2014 06:48 AM - Victor Julien
- Target version changed from 2.0rc2 to 3.0RC2

#13 - 05/20/2015 06:09 AM - Victor Julien
- Target version changed from 3.0RC2 to 70

#14 - 09/20/2017 04:41 PM - Andreas Herz

With rate_filter there is also a demand to override or combine the settings within the threshold.config and the used rules. This should match our documentation that when the ratelimit is reached the new_action should be applied and also needs to stay in that mode until timeout is reached. At the moment it's overridden by the threshold settings within the rule. (summary from discussion on the oisf-users ML with topic [Oisf-users] threshold.conf with rate_limit or drop rules in 9/2017)

#15 - 07/14/2020 01:25 PM - Victor Julien
- Status changed from Assigned to New
- Assignee changed from Victor Julien to Community Ticket
- Priority changed from Low to Normal
- Target version changed from 70 to TBD

Unclear what would be left to do currently. Leaving it to the community to submit more usecases that we don't support right now.

#16 - 04/28/2021 09:09 AM - Pavan Vachhani

Hi,
I came across this issue while reading the documentation. I am trying to apply threshold to limit the number of events generated by each rule/signatures. So, tried adding threshold.config as below but it seems it's not supported yet.

/etc/suricata/threshold.config
threshold gen_id 0, sig_id 0, type limit, track by_rule, count 1, seconds 10

/var/log/suricata/suricata.log

28/4/2021 -- 09:04:47 - <Error> - [ERRCODE: SC_ERR_PCRE_MATCH(2)] - pcre_exec parse error, ret -l, string , type limit, track by_rule, count 1, seconds 10
28/4/2021 -- 09:04:47 - <Info> - Threshold config parsed: 1 rule(s) found

I wanted to have a global threshold so that, logs aren't filled up with similar events from same signature in a short span like 10 seconds. Is there any other way to do this?
Thanks!