Prewikka - Support #1153

Suricata changes the output from version 4

11/07/2019 06:40 PM - Andrew Goldy

Status:	Assigned	**Start date:**	11/07/2019
Priority:	Normal	**Due date:**	
Assignee:	Andrew Goldy	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Resolution:			

Description

Hello Guys!

Suricata might has changed? the default prelude-alert output, because comparing to the old release 3.x the alert text was the alert name for example "ET POLICY Self Signed SSL Certificate (SomeOrganizationalUnit)", and now the alert text is swapped to description for example "Potential Corporate Privacy Violation".
Moreover comparing to snort its confirmed something was wrong with the alerting output at least in case of prelude in suricata.

Below the real world examples with the same alert from snort and suricata aspects. Both outputs are natively forwarded to prelude.
I've contacted suricata for months but still no answer... Is there any workaround to swap the two columns regarding suricata?

41 x **Potential Corporate Privacy Violation**		cloud.com	suricata
33 x **ET POLICY Self Signed SSL Certificate (SomeOrganizationalUnit)**		cloud.com	snort

Suricata:

Text	Ident	Severity	Type	Description
Potential Corporate Privacy Violation	1:2013659	**high**	other	ET POLICY Self Signed SSL Certificate (SomeOrganizationalUnit)

Snort:

Text	Ident	Severity	Type	Description
ET POLICY Self Signed SSL Certificate (SomeOrganizationalUnit)	1:2013659	**high**	other	Potential Corporate Privacy Violation

Many thanks! smile.png

History

#1 - 11/08/2019 09:12 AM - Camille GARDET

- Status changed from New to Assigned

- Assignee set to Andrew Goldy

Hello Andrew,

Thank you for reporting this.
In this case, it is the alert from Snort where the *classification.text* and the *description* are swapped. In the IDMEF format (and philosophy), the field *classification.text* should be as generic as possible, to ease the correlation.

We changed this behavior in suricata through this PR https://github.com/OISF/suricata/pull/3253 on GitHub.
If you are able to contribute to the Snort project by submitting a patch, it would be great. If not, we will look into it smile.png

Files

tempsnip.png	6.99 KB	11/07/2019	Andrew Goldy
ftzfztfztd.PNG	4.43 KB	11/07/2019	Andrew Goldy
jzff.PNG	4.29 KB	11/07/2019	Andrew Goldy