This could probably become more than just one ticket.
The motivation behind it is that there are many rule keywords
that are mentioned but lack proper explanation on what they are/
how they related to what is seen on the wire.

Improving that would be great.

Subtasks:
Documentation #5385: userguide: update rule's format document - Closed
Hello JT, thanks for your input!

In general, I think we try to avoid adding images and diagrams when we can, for the reason you just pointed out: they tend to get outdated and are harder to change and maintain than code/text.

From my experience, when we do think diagrams are needed, we have been trying to move towards images or representations that are easier to maintain and update (for example, diagrams that were generated from a text schema: https://suricata.readthedocs.io/en/latest/devguide/extending/app-layer/transactions.html#sequence-diagrams).

But I understand that is not always feasible, so it's a trade-off between how much effort it would be required to find a more maintainable solution, and the time you have available for the task.

To summarize:
- images are not mandatory
- we prefer to have alternatives that can be autogenerated and are easier to update and track when we do have images

(I hope this answered your questions!)

#4 - 05/10/2022 08:46 PM - Jason Taylor

Juliana Fajardini Reichow wrote in #note-3:

Jason Taylor wrote in #note-2:

I was looking at the http keyword docs at https://suricata.readthedocs.io/en/latest/rules/http-keywords.html and it got me wondering what the best way to display some of the data is?

Some of the pictures in this case, method.png, is being used to illustrate the GET method and keyword usage. In this case the paragraph above the image mentions http.method but the picture references http_method.

I wonder if this sort of scenario is confusing to new rule writers?

I can see that happening - we do mention that there are newer versions of the keywords in other, so hopefully although not ideal, not so harmful we'd have to remove them altogether.

Is there an alternative to images that we would want to consider?

I ask because before starting to document new keywords, I am curious if how things are currently layed-out/explained are what we want to continue with?

Thanks in advance!

JT

Hello JT, thanks for your input!

In general, I think we try to avoid adding images and diagrams when we can, for the reason you just pointed out: they tend to get outdated and are harder to change and maintain than code/text.

From my experience, when we do think diagrams are needed, we have been trying to move towards images or representations that are easier to maintain and update (for example, diagrams that were generated from a text schema: https://suricata.readthedocs.io/en/latest/devguide/extending/app-layer/transactions.html#sequence-diagrams).

But I understand that is not always feasible, so it's a trade-off between how much effort it would be required to find a more maintainable solution, and the time you have available for the task.

To summarize:
- images are not mandatory
- we prefer to have alternatives that can be autogenerated and are easier to update and track when we do have images

(I hope this answered your questions!)

It did, I will put together a PR to get your thoughts and we can go from there. Thanks! (Sorry for the delayed response, I didn't get a notification the ticket got updated, I forgot to watch this :)).