Analytics Research Report

Background

In the pursuit of improving the analytics rule area in Axon, research was conducted on the current experience and possible improvements via user interviews and a survey, with the output of this report being improvement recommendations. While we are focused on general improvements in both the overview page and rule builder areas, some specific feedback was also requested around search and organization on the overview page and rule suppression. Below are recommendations and links to supporting data.

Opportunities & Recommendations

A lot of very valuable data came out of the four user interviews and a survey that was posted on Pendo (5 results). Below is a list of improvement recommendations based on the feedback. For more information about each option, please select the link to view the associated highlight.

Small Wins - minimal UX and engineering effort

Rule builder

- substantially increase description field length - users tend to put in use cases, links, and other resources in this field so analysts have something to reference when an observation is created
- add suppression in attributes tab - in discussions with users, there seemed to be two camps of how users want suppression to work. If a rule was triggered 10 times in 10 minutes, users either want (A) only create one observation and send one notification or (B) create ten observations but only send one notification.

Overview page

- data grid improvements - search (filter options and data available) and table actions
    - allow users to group and filter on all columns in the analytics grid. This is the easiest and quickest way for users to find the data they need and group things accordingly.
    - add more data into the grid
        - rule last updated
        - rule last triggered
        - how often rule is triggering in x timeframe
        - author - this should show a specific user and not only the tenant
        - auto case status - enabled/disabled
        - suppression - timeframe
        - severity

        - unique ID - surface an uneditable rule ID that folks can use when discussing rules. Rules can look similar except for small details so having this will help ensure users are talking about the same rule when collaborating

- improve grid bulk edit options
    - enable/disable auto case creation
    - view multiple rule outputs (mixed reviews on how to implement this from users - one wanted to show all outputs in one search vs another wanted each rule to have it's own search)
    - export rules
    - retire rules
- ability to export a CSV file of the analytics grid - this is helpful when folks are requested to share current or possible coverage with clients and other members of their organization

Larger Work Items

Rule Builder

- mapping link group by options - more research should probably happen before implementing this but users stated it would allow for more use cases that currently aren't available when search queries are confined to a single block
- "log not observed" rule block - the need for this was expressed by several users and would greatly improve the amount of use cases we can cover
- improve query filter UI to make it easier to read and edit - this ties into improving rule builder UI to more effectively use space
- general UI improvements - add more information on group bys and metadata field, rethink the UI layout of elements and workflows

Improvements outside of rule area

- show rule logic in observation generated - it would be helpful if users are able to easily see rule logic in the observation panel like you can in LR SIEM rather than need to navigate into the rule builder
- allow users to take a search and convert it into an analytics rule - searches are hard to build and would be helpful to take searches that are already created (ex. from threat hunting) and easily write an analytics rule off of that use case