How to Validate the entities versus the Automation Rule

Last updated by | Naser Mohammed | Mar 19, 2023 at 7:18 AM CDT

Note: Adding this section after spending over 80 days on 2210270040006096 when this solution would have saved several weeks.

Background

On this case, the customer had created an Automation Rule, it was not picking up the proper entity "command line" according to the instructions on this other wiki page.

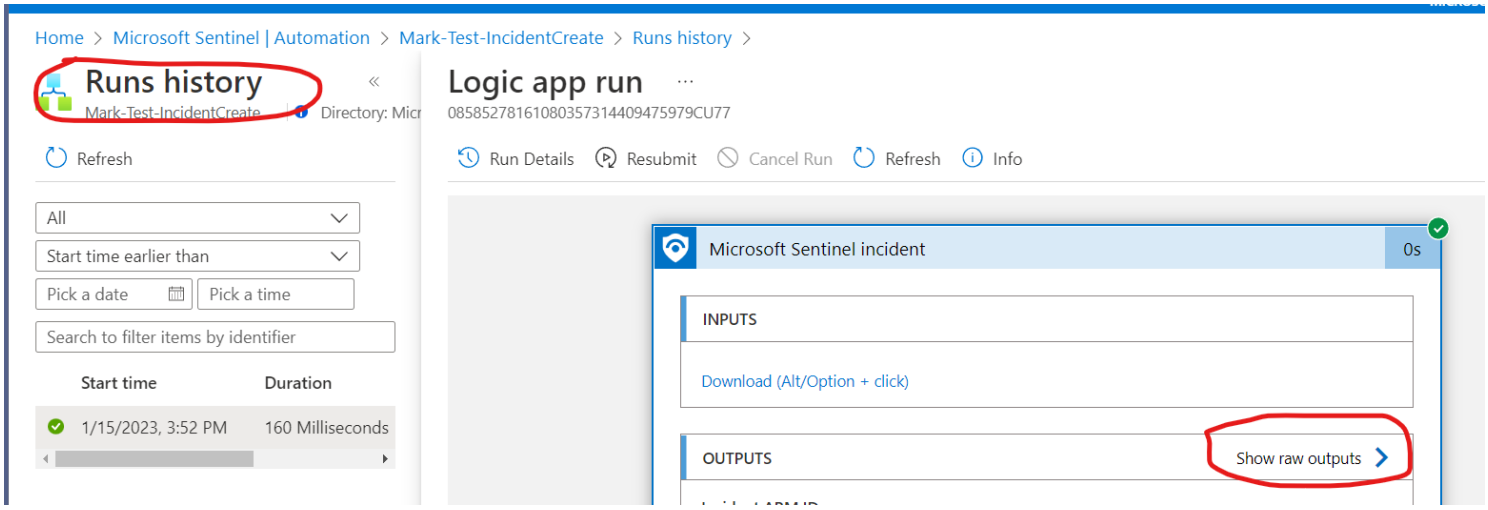
What happened was that the command line in Log Analytics would show up as: "net user", but in reality the command line had a double space: "net user". And, the Log Analytics would clean up the entities to show it as simple text. Therefore, not even with the assistance of PG we were able to catch the difference until PG suggested the following method.

Use Automation to catch the Entities details

Per the ICM a new LogicApp Playbook may be created along with a new automation rule with the minimum conditions so that it will catch the incident. Then, point the new automation rule to run the plain playbook, this will catch the raw data before it even makes it to the Log Analytics workspace.

Steps:

1. Create a new LogicApp Playbook with Microsot Sentinel, using the "Microsoft Sentinel Incident" trigger. Do not add more blocks to the logic app. Save it.
2. Create a new Automation Rule with one Action: Run playbook, and select the previously created playbook.
3. On said Automation Rule configure the filters to have the same conditions that are not related to entities, meaning, select the appropriate Analytic Rule. If you've followed the wiki page and have confirmed that the issue is only with certain entities, then you can specify the entities that do not show an issue.
4. When the next incident happens, go to the Logic App, and check for the Runs History.
5. Select one or several of the runs, and from it, click on Show Raw Outputs.
6. Inspect the JSON output for the entities. In here, the text will not have been processed and you may be able to find possible errors or issues on the text with which the entities are coming into Log Analytics.
7. Remember to delete the Logic App and the Automation rule created with these steps once the issue has been corrected.


Home > Microsoft Sentinel | Automation > Mark-Test-IncidentCreate > Runs history >
Runs history
Mark-Test-IncidentCreate
Directory: Micr
Refresh
All
Start time earlier than
Pick a date
Pick a time
Search to filter items by identifier
Start time
Duration
1/15/2023, 3:52 PM
160 Milliseconds
Logic app run
08585278161080357314409475979CU77
Run Details
Resubmit
Cancel Run
Refresh
Info
Microsoft Sentinel incident
0s
INPUTS
Download (Alt/Option + click)
OUTPUTS
Show raw outputs