M365D connector - Log counts discrepancy between M365D tables and Sentinel tables

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

Issue Description: Customer has M365D connector set up and they would like to know why they are seeing Log counts discrepancy on the AlertEvidence Table between advanced hunting in M365 and Sentinel workspace.

For example, running the following query against the same time period (past month) from both M365 and Sentinel workspace.

```
AlertEvidence

| where Title == 'Custom TI: Detection of remote access tool in conjunction with Unblock-File command'

| distinct AlertId
```

In Sentinel workspace less results than running in M365D

Expected result: There should be 1-to-1 parity in logs based on this doc: https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-alertevidence-table?view=o365-worldwide

Cause:

Somewhere around the 23'th of Jan, PG pushed a change to the code that aligned the M365D tables with Sentinel tables. (the connector was not in GA end of January so there were some fields missing - not its GA) What happened is that the "Title" column didn't exist in the Sentinel schema up until the 23'rd - starting from the 23'rd the title's started to show up.

Running this query on the customers data will show this clearly :

```
AlertEvidence
| summarize count() by Title,bin(TimeGenerated,1d)
```

So we would expect that if you compare all events in M365D and Sentinel events (Regardless title) you would see a 1-to-1 correlation. and starting from the 23'rd you should see a 1-to-1 correlation even when grouping by title.

Reference ICM: https://portal.microsofticm.com/imp/v3/incidents/details/369946276/home