Microsoft Defender for Cloud Apps (MDCA, MCAS) data connector

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

McasShadowItReporting Table (Data coming from MDCA Cloud Discovery)
https://learn.microsoft.com/en-us/azure/azure-monitor/reference/tables/mcasshadowitreporting

-- **TimeGenerated Column has records with same timestamp** (by design)

- Customers might be confused by the TimeGenerated value of the records in this table. The timestamp will have all records with the same time for a specific date.
- The TimeGenerated column is specific to the source that it comes from.
- The time continues to be rounded specific to the date column during the enrichment process to MDCA SaaS database.
- So the backend doesn’t even look at the timestamp. It is specific more to the day inside the logs.
- MDCA does allow the forwarding of these logs to the sentinel environment so customers can make their own dashboards/data triaging.
- However, during the enrichment process of these logs for MDCA dashboard under cloud discovery, MDCA continues to set these logs specific to the date.
- It wasn’t built to be specific to the exact timestamp of when the event happened.
- These logs were mainly used just to show what applications are being utilized on your environment from a shadow IT prospective, allowing you to take action on them.

  Source: MCDA Escalation Engineer respopnse, Case# 2205300040005960