

NRT Rules

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

[NRT Rules General Information](#)

- By design running every 1 minute with 1 minute lookback period
- The use Ingestion_time() instead of TimeGenerated
- No more than 20 rules can be defined per customer at this time -You cannot use unions or joins

Important Limitation

NRT rules cannot be used with a function table. If this is done it will result in the creation of much more alerts than expected. [lcm](#) 