New AMA based Windows Security events connector -TSG

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

Please use the following troubleshooting steps :

- Please validate customer is using the new AMA agent and that the machine is sending heartbeat, by running :

Heartbeat | where TimeGenerated >= 1h | where Computer == "[Computer name]" | take 10

- Ask the customer to provide the Data Collection Rules that he's configured (if any). It can be found in the "Configuration" section of the connector page.
- Ask customer to provide a sample of the missing events or the Xpath that he's configured from the Event Viewer. Try to reproduce the issue with given data from customer
- If Security Center is also installed, please check if customer also configured security events collection from there.
- 1st ingestion may take up to 20 minutes
- When customer update the Xpath, it will only work for new events, meaning that it will not update the existing data.