

Ingestion Delays

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

Contents

- [Sentinel Alert Ingestion Delay query](#)
- [Sentinel Incident Delay queries](#)
 - [Notes:](#)
- [MDE Device Events Delay](#)

Sentinel Alert Ingestion Delay query

```
SecurityAlert
| where ProductName == "{ProductName}"
| extend SourceProviderLatency = ingestion_time() - TimeGenerated
| extend SentinelLatency = TimeGenerated - ProcessingEndTime
| project SystemAlertId, DisplayName, SourceProviderLatency, SentinelLatency, _TimeReceived
```

Sentinel Incident Delay queries

```
SecurityIncident
/// where ModifiedBy == "Incident created from alert"
| extend IncidentIngestionLatency = ingestion_time() - TimeGenerated
| project TimeGenerated, ingestion_time(), IncidentIngestionLatency, AlertIds, IncidentNumber, ProviderIncidentId
```

```
SecurityIncident
| where IncidentName == ""
| project TimeGenerated, TimeReceived=_TimeReceived, IngestionTime=ingestion_time()
| extend delayUntilLAINSeconds = (TimeReceived-TimeGenerated)/1s, delayInLAINSeconds=(IngestionTime-TimeReceived)
```

Notes:

ingestion_time(): when it was written to Kusto and available for query (LA)

TimeGenerated: set by Sentinel when the incidents was updated (US)

_TimeReceived: when it reached ingestions pipeline of LA (Scuba)

The two value have the following relationship: **ingestion_time() > _TimeReceived**


If the ingestion_time() and _TimeReceived do not have any delay, then the delay is most probably with the provider.

The above queries can be used for all 1st Party Connectors (DeviceEvents.. etc)

MDE Device Events Delay

If the issue is about Device Events delay from the M365D Connector, a quick way to identify where the issue might be is the following query:

```
cluster('https://wcdprod.kusto.windows.net').database("Geneva").InvestigationMachine('<DeviceId>',-8d,0d,1h)
```



When executed for a specific DeviceId (can be extracted from Device Events) it shows how often the machine is communicating with the MDE cloud. If there is a delay (a gap), the issue is 100% with MDE and not with Sentinel

Example query: Dynamics365Activity | where TimeGenerated between (datetime(2022-04-28 18:00:00) .. datetime(2022-04-28 20:35:00)) | extend IngestionLatency = ingestion_time() - _TimeReceived | extend ReceiveLatency = _TimeReceived - TimeGenerated | summarize percentiles(IngestionLatency, 50, 95, 99), percentiles(ReceiveLatency, 50, 95, 99) by bin(TimeGenerated, 6h) | order by TimeGenerated

-> have LAW team look at first always -> then look at scuba/sentinel icm