Good to know stuff

Last updated by | Hekmat Abuzahrah | Mar 30, 2023 at 8:35 AM CDT

M365D connector not recognizing MDE license :

The customer can connect the M365D connector only if his MDE license is on the same tenant

Azure function :

My customer want to enable Salesforce connector in Sentinel. Our question is if Salesforce connector could connect multiple Salesforce instances or one Sentinel Workspace only could collection one instance logs.

A connector (in turn azure function) deployed will take a function name, SalesForceTokenURI and corresponding credentials that will pull the data and ingest into Sentinel. One way of supporting multiple instances can be achieved by installing the connector (azure function) multiple times with different names (different instances of azure function) with each function pointing to one instance.

Documentation for API: https://developer.salesforce.com/docs/atlas.en-us.api_rest.meta/api_rest/quickstart.htm

TAXII :

We have two questions about Threat Intelligence indicator: • Could we set expired time for feel ree threat intelligence indicator. From the screenshot we can see there is no valid until date.

If we add new indicator from portal directly, we can set the valid until date, so customer want to know if we can set the expired date from indicator collected by Threat Intelligence Platforms connector as well. [Rijuta]: We currently do not allow editing of indicators brought in from 3P sources, so indicators you get from the TIP and TAXII connector are not editable. With that being said, we are working on releasing a new feature in the next few weeks by which you would be able to edit indicators coming from 3P sources as well using the “3 ellipses” on the right of the indicator grid. Also, in [Cu] we are working on a feature where in you can create rules that will take actions on indicators satisfying that rule and Edit is one of the available actions. For example, you can create a rule saying all indicators that come from the Source as “FS-ISAC” set their Valid Until date to “2022-10-10 00:00:00”.
• About ThreatIntelligence table column: See this example, in the portal, it shows the ‘Name’ field that is populated.

But in the ThreatIntelligenceIndicator table, we don’t seem be able to see this field at all. I have checked the document about ThreatIntelligenceIndicator table, from the reference seems the ‘name’ doesn’t exist in the column, may I know if name information cannot be shown understand this table?

Reference link: Azure Monitor Logs reference - ThreatIntelligenceIndicator | Microsoft Docs

[Rijuta]: Name is currently not a part of the ThreatIntelligenceIndicator table schema in LA. The TI blade is actually populated of a separate storage we have which is Cosmos DB and Name is part of the Cosmos DB. With that being said, in [Cu] we are adding the Name field to the LA table as well.

Watchlist :

LA has a 5 minute SLA for ingestion.

Deleting and recreating a watchlist will result in data ingestion for both a) deleting the old entries and b) populating the new entries and also result in an update to our Cosmos DB.

So there is a very good chance that you can see both results in LA within this 5 minute window. This won't happen in the watchlist UI since the UI is not reading from LA but is reading the data from Cosmos DB.

SAP connector :

Troubleshooting guide https://docs.microsoft.com/en-us/azure/sentinel/sap-deploy-troubleshoot Microsoft Sentinel SAP solution deployment troubleshooting

Customer is integrating the SAP solution with Sentinel following this guidance: https://docs.microsoft.com/en-us/azure/sentinel/sap-deploy-solution#deploy-a-linux-vm-for-your-sap-data-connector Basically, this solution is to install a docker in an Azure VM as the agent to stream data from SAP and to Workspace. The questions are:

1. The customer have many SAP systems , can we build the connectors in one VM? Or we need to build up different VMs for different systems? Answer : 1. Currently the architecture is one docker per sap system, We are considering changing this for future releases.

2. Also customer's SAP Server is internal server , how they can talk to Azure, do we need a gateway or something else? Answer : 2. The Docker need to have a connection open to Azure Via gateway, proxy etc.., This is a done per customer security standard.

Multi tenant support :

- AAD doesn't support multi-tenant yet

Workbooks :

- Workbook updates - Usually minor version bumps (1.1 to 1.2) are bug fixes or small additions. The 1.0 to 2.0 version bumps are usually major changes, like addition of tabs or breaking changes

UEBA

- Missing data in PeerAnalytics table : This is by design. Since we run batch processing jobs, on Jan 31st at 10 pm we published data for Jan 30th We ask customers to query for at least one week of data for user peer analytics tables Table owned by SIPs ML

- Identity info is updated when we saw any change in the "ID" of the user in AAD, for example - his name was changed, changed manager, added to a group, granted a role etc, the update may take up to 15 minutes after the change in AAD

Events like sign-in won't be gathered in this table since they are not reflecting a change

- I have a customer who's experimenting with UEBA and has an issue with the IdentityInfo table not showing any data although all other data sources are showing data and other UEBA tables are showing data up to date. I believe this table is in preview so I was just trying to provide as much help to the customer and maybe we can get more information about it since there's no documentation anywhere about this table.

The questions is:

```
1- What exactly is the flow of this table and what data source does it use exactly?
```

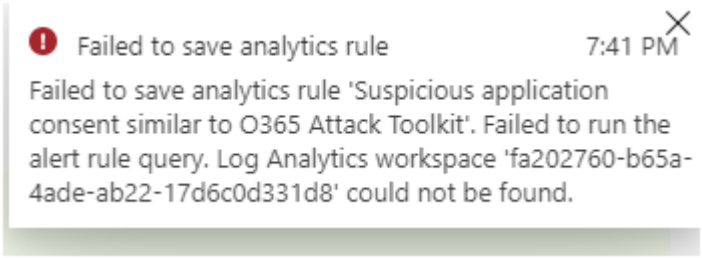
Once customer is onboarded to UEBA- UEBA engine starts syncing entities from AAD and and push those (via integration with scuba EHs) into LA identity info table. In the future we will add additional dynamic attributes to this table to give better context (beside the static attributes we're pulling from AAD) 1- What could be a reason for the data not be shown on the table? This feature is on pp- this means that in order to enable this feature we (dev team) need to onboard the customer manually. Please share customer WS id if customer would like to join the pp.

- Lower amount of UEBA data :

This may happen when we perform maintenance operations in the system backend. As long as the time frame is relatively small (~less than an hour) the behavior is expected.

General

- Overview page issues : Getting an ERROR while enabling the Analytics rules



we are caching the workspace id's for a week (after deletion).

Incident

- bi-directional incident integration is supported only when using the M365D integration.

One-directional sync, meaning from the source to Sentinel, is supported for all 1P alerts providers (MDI, MDO, MCAS, AzD, MDE). If you close an alert in any of those product, we will present the alert in Sentinel as closed, but it will not affect the incident

- About alert closed and incident he corresponding incident in Sentinel gets modified but does not gets closed:

Alerts from other providers such as MDI , MCAS & ASC are different Entities then Sentinel's incident. You can observe That once alert is closed in other provider you can see the the sentinel incident was updated (and the alert inside it is closed), but the incident itself wouldn't be close

- Delay that > 30 mins between alert and incident

We have logic that that cover ingestion latency issues in LA: For each query run, in case an alert was NOT published, the query will run again in ~30 min to cover case of event ingestion delay.

When our background service run the query for the first time,it found 0 results -> alert was not published -> ~30 min after it run again and found the data -> alert was created -> incident was created.

Example - Let's say the event was created on 8:00 on the machine itself but was ingested into LA in 8:07 (network delay or any other traffic).

The rule that ran ~ 8:00 / 8:05 will miss this alert, but it will initiate a new query that will run on same timeframe in 30 minutes later, so in 8:30 the query will run again but now it will find this event (therefore you would see this delay)

You won't get this event from the run of 8:10 because the actual generated time is 8:00 (we don't check the ingestion time).

- https://msazure.visualstudio.com/One/_workitems/edit/9424148

When we are calling the investigation service, like "get entities" command, we send the customer data in the headers. if customer's data has some non-asci characters, it will fail.

For example - "ResourceGroupName":"持出pc“

Alert rule

- Alert rule return missing fields : Check if the customer used 'take' operator in his query - as a result the returned rows are not consistent between different query executions. (Because take is random).

In our service, when a windows of the rule is running (each X minutes\hours as defined by the customer) we're running the query twice.

Firstly to check whether the amount of returned results in order to compare it to the threshold operator and threshold, and if the condition is met, we're running again to get the actual data.

As you can see, using the 'take' operator is problematic because of its randomicity.

The first (count) query returned results, and the condition is met because user set to create alert when number of rows greater than 0.

But the second query run returned 0 rows, and that's why there were zero entities in the resulted alert.

- An Analytic Rule failed to execute : run this query to find more data :

//Analytic Rule Executions let startDateTime = datetime(2021-5-23 00:00:00.0000000); let endDateTime = datetime(2021-5-26 00:00:00.0000000); ServiceFabricDynamicOE | where env_time between (startDateTime .. endDateTime) | where serviceName contains "AlertRulesApp" | where resultType != "Success" | where operationName =="Security.Insights.AlertRules.ScheduledAlertRuleConditionCheckerActor.AlertTriggers.ThresholdAlertRuleConditionChecker.IsRuleConditionsMetAsync" | where customData contains "0c358c63-864c-4b90-a34d-9a140070c9ff"//rule id

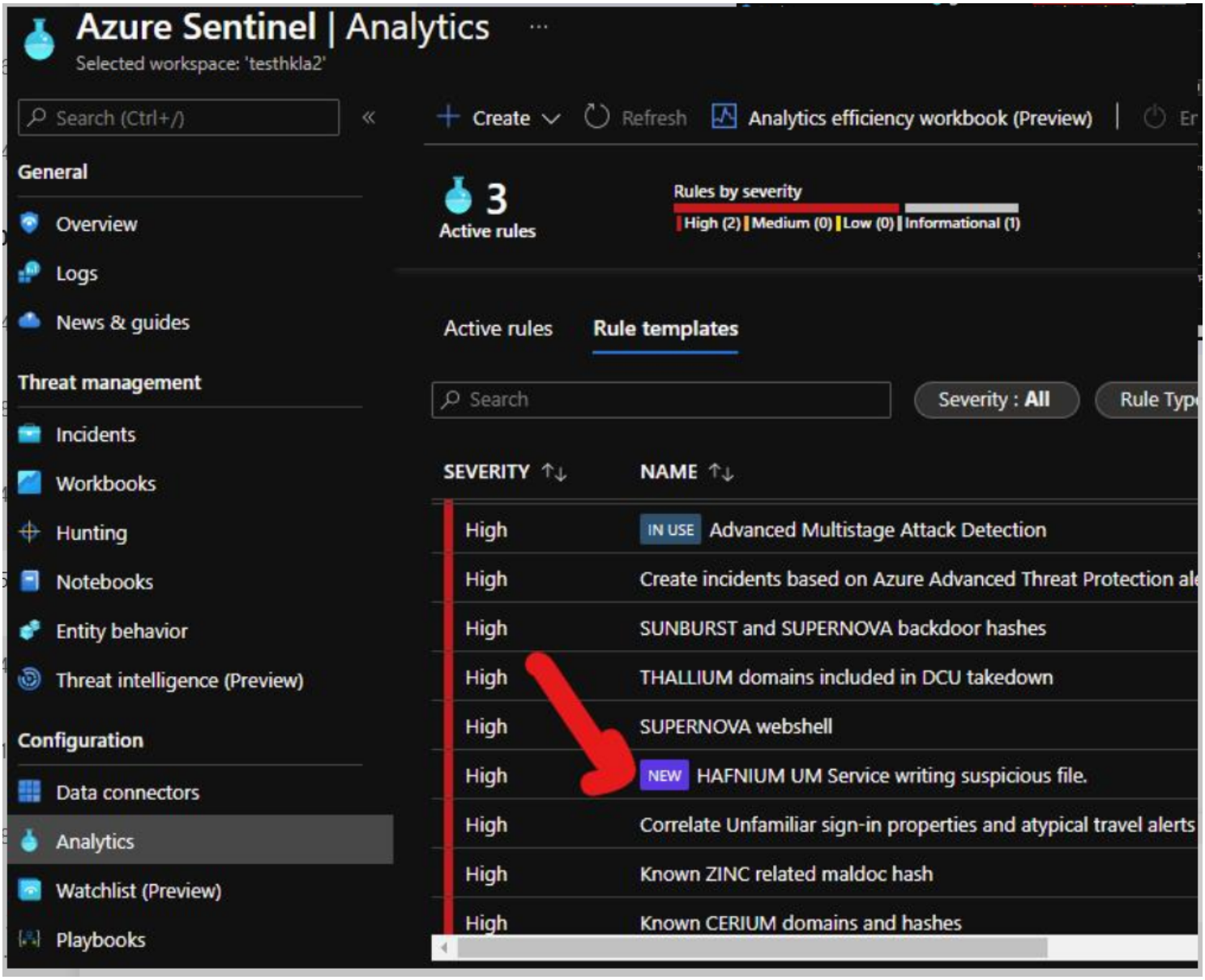
- Missing ATP alert - (also log is missing) Check that alert size is smaller than 64kb, currently it's LA's limitation :

Execute in [Web] [Desktop] [cluster('securityinsights.kusto.windows.net ').database('SecurityInsightsProd')]ServiceFabricDynamicOE| where env_time > ago(5d)| where applicationName contains"alertgateway"| where * contains"MISSING-ALERT-ID"| limit 10 (replace alert ID)search results for "OriginalMessageSize" and "MessageSizeAfterTrim"

- Handling ingestion delay in Azure Sentinel scheduled alert rules

- Analytics Rule Running Twice Instead of Once - check if customer manually changed the rule - it will reset the scheduling and will trigger the alert

- "NEW" flag in Analytics rule :



will be shown for fixed 14 days

- Entity grouping problem

The customer's query returned more than 20 rows, so we created an alert for each row for the first 19 rows, and then grouped the rest of the events into a single alert - which contained more than one host.

Currently the number of alerts a rule can generate is capped at 20. If in a particular rule, Event grouping is set to Trigger an alert for each event, and the rule's query returns more than 20 events, each of the first 19 events will generate a unique alert, and the twentieth alert will summarize the entire set of returned events. In other words, the twentieth alert is what would have been generated under the Group all events into a single alert option.

This behavior is by design.

Data

- connecting connectors which are in preview via the PowerShell won't work as expected, bug was created for that.

- DNS Inventory data :

DnsInventory table Unlike DNS events, DNS inventory data is not a continues data flow, rather a simple powershell script that runs once every two days and takes a snapshot and sends it to the customers workspace. Data can be received with a delay of upto 2 days

- CEF

start time and end time fields are not supported, will contains null, this is by design in the Workflow

- Disconnect connectors :

Connectors configured in Sentinel show connected/disconnected immediately Connectors configured outside show configured while there are 2 weeks (14 days) of recent data"

- Sentinel does not support AWS-GovCloud at the moment
- Missing fields in AzureDiagnostics - see here Some columns will not exist if there was no data for them at any point in time. The action_s column will appear in the schema only if at some point such data was ingested. At the time of ingestion that column will be created in the schema. Moreover, certain columns are created only when first data for them arrives.
- connectors mapping
- Missing events (less than expected) for specific timegenerated :

OfficeActivity

| where TimeGenerated > datetime(2021-1-20) and TimeGenerated < datetime(2021-1-21)

| where RecordType == 'SharePointFileOperation'

Customer didn't use ">=" and "<=" and we found the missing logs are from 00:00 so they won't be gathered for this query

- Duplicate Events from Multiple Log sources

cx has thousands of alerts, duplications are expected, the nr of duplications is below the threshold, confirmed by PG (by design) 4 duplications which are 0.01% of their alerts. this is reasonable and should not raise any concerns.

PR / PP

- Sentinel logic app trigger connector for incidents

Public preview – upcoming 2-3 weeks (together with Automation Rules). We announced Automation Rules in Ignite and the feature will be up officially this month. GA – no ETA at the moment.

Data Retention of ML features

Out of all Azure ML features only the analytics rule type "ML Behavior Analytics" sends data across geos in some regions as stated in our documentation. However for EU customers "ML Behavior Analytics" is deployed in

EU, i.e. data in EU stays within EU.