Indicator in Log analytics

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

Issue 3:

Rule is enabled and incidents are being generated but the indicator is not available in the ThreatIntelligenceIndicators Log Analytics table

Step 1: If the customer has enabled the rule and is seeing alerts and incidents being generated from the rule but is not able to find the matched indicator in LA, use the following query to validate that the indicator is not in LA :

The time range has to be a bit more than a month because we do not send the same indicator over and over (with each match). An indicator will expire from LogA in a month, so we have to select with a time range of at least one month. Setting it to 32 days to make sure we got the whole window.

Note: Running the query without a time range, will allow the editor to pick a time range and that is by default 7 days.

> ThreatIntelligenceIndicator
>
>> where TimeGenerated > ago(32d) and SourceSystem == "Microsoft Threat Intelligence Analytics"

If the query returns results, then walkthrough the customer with the process of searching the indicator in LA . If the query does not return any results open an ICM mentioning the issue and relevant screenshots.

> Needed details:
>
> 1. WorkspaceID or Workspace Name
> 2. Time or a time window when the rule was enabled.
> 3. Reason why alerts are expected to appear (i.e. which 'observable' is expected should have matched).

Note : ICM should be opened on the following team : Owning Service: Sentinel US Owning Team: Threat Intelligence

Note: This analytics rule runs every 15 mins.

SLA for Issues:

- Sev3/Sev4: Within 1 complete business day (for acknowledging the issue). The actual resolution time for the issue will be longer on a per issue basis.
- Sev2: 5-10 mins of acknowledging. The team will work on the issue until it is actually resolved.