Rule Not Enabled

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

Issue 1:

Rule is not enabled and is not showing in Active Rule tab for Analytics

Verify the rule is enabled using the following steps:

1. Open the Azure Portal and navigate to the Azure Sentinel service.
2. Choose the workspace where you've CEF Logs flowing in.
3. Navigate to the "Analytics" section under the Configuration pane.
4. Under the Active Rules tab search for "Microsoft Threat Intelligence Analytics". Make sure that the rule is showing up there.
5. If the rule is not showing in Active Rules, go to Rule templates and search for "Microsoft Threat Intelligence Analytics" (you could filter first by Rule Type = "Threat Intelligence". Highlight the rule template and click on the "Create Rule" button in the summary panel. Make sure the Status is set to "Enabled" and click "Next: Review", then "Create".
6. If the rule is present in "Active Rules" tab, highlight it and make sure it is enabled.

If it isn't you can enable it from the context (right-click) menu.

If you still do not see matches come through (after 40 minutes) open an ICM with details of the issue and relevant screenshots. (Details to open ICM are below)

> 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.