Alerts or Incidents not generated

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

Issue 2:

Rule is enabled but no alerts/incidents are being generated with matches from TI Indicators

Validate the rule is enabled, following these steps.

If the rule is enabled and alerts and incidents are not being generated: Make sure that CEF logs are flowing into this workspace and the Request URL Field is mapped correctly:

> Check if there are any 'valid' logs received in the past hour CommonSecurityLog
>
> > where TimeGenerated > ago(1h) and not(isempty(RequestURL))

If there are no log events that have empty RequestUrl, take a look at the value verify it is a reasonable URL, by removing the and clause:

> CommonSecurityLog
>
> > where TimeGenerated > ago(1h)

If the CEF logs are also mapped correct then the matching analytics should be working fine. Do a similar check for Syslog and DNS logs. If you see additional issues please create an ICM mentioning the issue with 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.