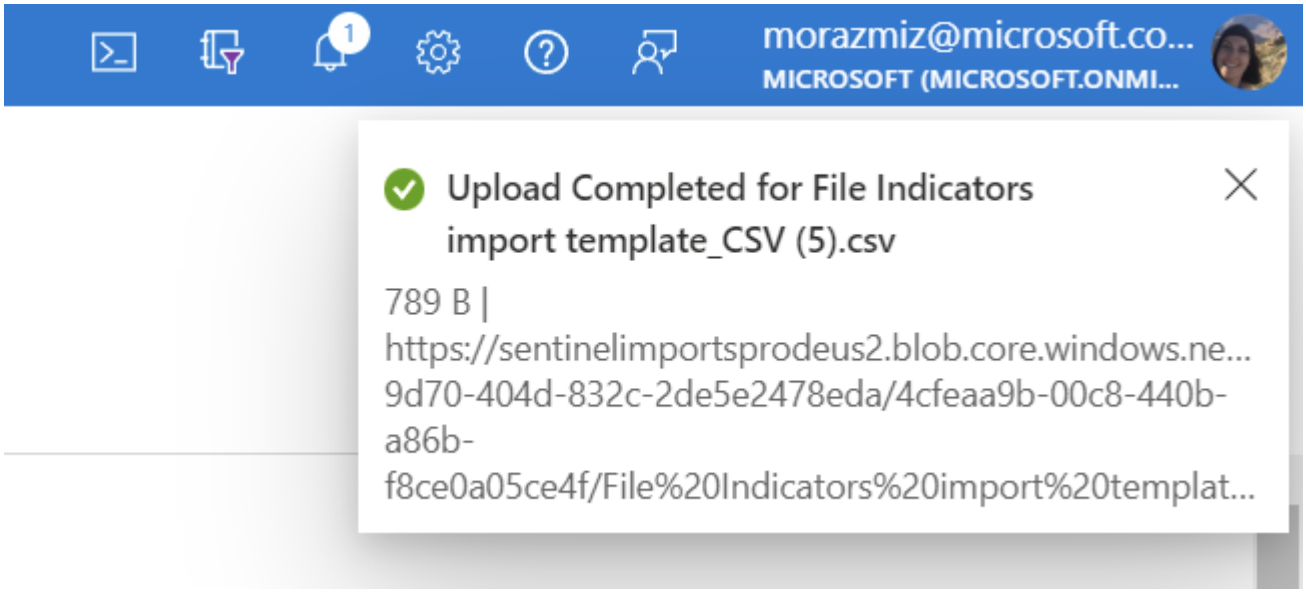
Common issues troubleshooting 2

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

Issue 2: The file seems to have been uploaded but the indicators are not yet available

Option 1: If a customer complains that they saw the following notification:



But that their indicators are not yet showing in Sentinel - this is normal. The above notification only means that the file was successfully uploaded, but it does not mean it was successfully ingested into Sentinel. To check the ingestion status, please go to "manage imports" and check the status of your file. You will often see that the file is still in status "in progress".

Option 2: If the file is marked as "fully ingested" / "partially ingested" in the "manage imports" blade, but the user still can't see the indicators they imported in the indicator grid: Sometimes it can also take some time for the indicators to show on the indicator grid after the file was successfully ingested. A rule of thumb is about 5 minutes or so. If this time has passed and the indicators are still not available, open an IcM with the following information:

1. include the file id. Go to this page to learn how to find the file id.
2. Mention if the indicators are not available both in Sentinel and in Log Analytics, or just in one of them. You would have to ask the customer to provide this information. In order to find out if the indicators made it to Log Analytics, the customer could go to "logs" and run the following query: ThreatIntelligenceIndicator | where TimeGenerated > ago(7d) // change this to include the time the file was imported) | where SourceSystem == "fileName" // change this to the source of the file (you can see what it is in the "manage imports" blade)

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

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.