Threat Intelligence Matching Analytics

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

The Threat Intelligence Matching Analytics enables Azure Sentinel customers to receive alerts and incidents generated by matching Microsoft generated Threat Intelligence Indicators with their own logs. The customers also obtain a copy of the matched indicator from Microsoft to use it for Hunting and Investigation.

This feature is currently in Public Preview and has the following pre-requisites : 1. Participants should be bringing in CommonSecurityLog, DNS logs, Syslog into their workspaces.

Troubleshooting Azure Sentinel Threat Intelligence Matching Analytics

Issue 1: Rule is not enabled and is not showing in Active Rule tab for Analytics

Issue 2: Rule is enabled but no alerts/incidents are being generated with matches from TI Indicators

Issue 3: Rule is enabled and incidents are being generated but the indicator is not available in the ThreatIntelligenceIndicators Log Analytics table

Contact @<97115010-11D2-6BAC-8A64-985EB42AE0B3> or **@O. Militao** for any modifications on these documents to make sure above provided links are not breaking wherever it's calling for a reference