

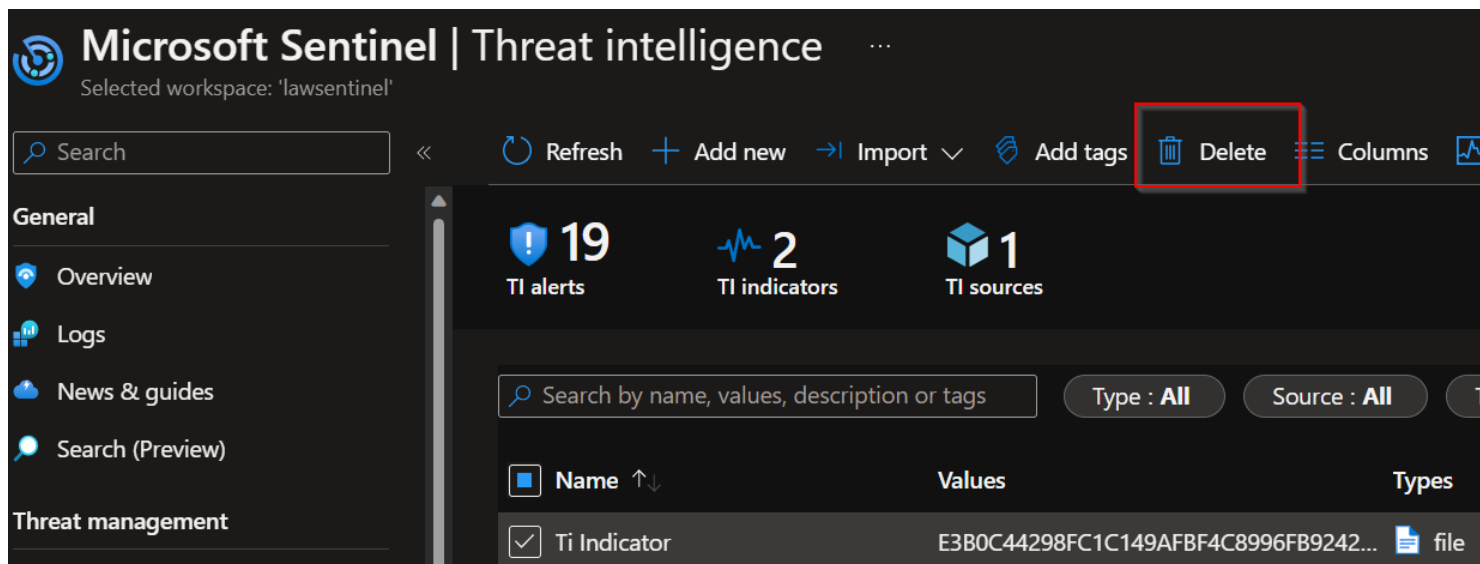
Delete-Threat Intelligence Indicator

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

Using API to bulk delete:

- To use delete API you would need name of the TI Indicator. which you can get using api : [Threat Intelligence Indicator - Query Indicators](#) ☞
- use API [Threat Intelligence Indicator - Delete](#) ☞ to delete Indicators.

Manually deleting TIs



The screenshot shows the Microsoft Sentinel Threat Intelligence dashboard. The top navigation bar includes a search bar, a refresh button, and buttons for 'Add new', 'Import', 'Add tags', 'Delete' (highlighted with a red box), and 'Columns'. Below the navigation bar, there are three summary cards: 'TI alerts' with a count of 19, 'TI indicators' with a count of 2, and 'TI sources' with a count of 1. A search bar is present with the placeholder text 'Search by name, values, description or tags'. Below the search bar, there are filters for 'Type : All' and 'Source : All'. A table is displayed with columns for 'Name', 'Values', and 'Types'. The table contains one entry: 'Ti Indicator' with a value 'E3B0C44298FC1C149AFBF4C8996FB9242...' and a type 'file'.

FYI

- Creating and/or deleting each indicator will create a log entry under table **ThreatIntelligenceIndicator**
- Graph api <https://learn.microsoft.com/en-us/graph/api/tiindicators-post?view=graph-rest-beta&tabs=http> ☞ are used to create TI indicators on Target products (Azure Sentinel, Microsoft Defender ATP). But all delete threat intelligence indicator graph api seems to be not ready to delete TI indicators from sentinel yet. From my test, Delete API does not support "targetProduct" parameter and by default it will try to delete TI indicators from MATP. Error while trying to delete sentinel TI indicator using graph api
"**Warning**': '199 - \'Microsoft/Microsoft Defender ATP/405/7\',199 -
'Microsoft/Interflow/400/390\'',"