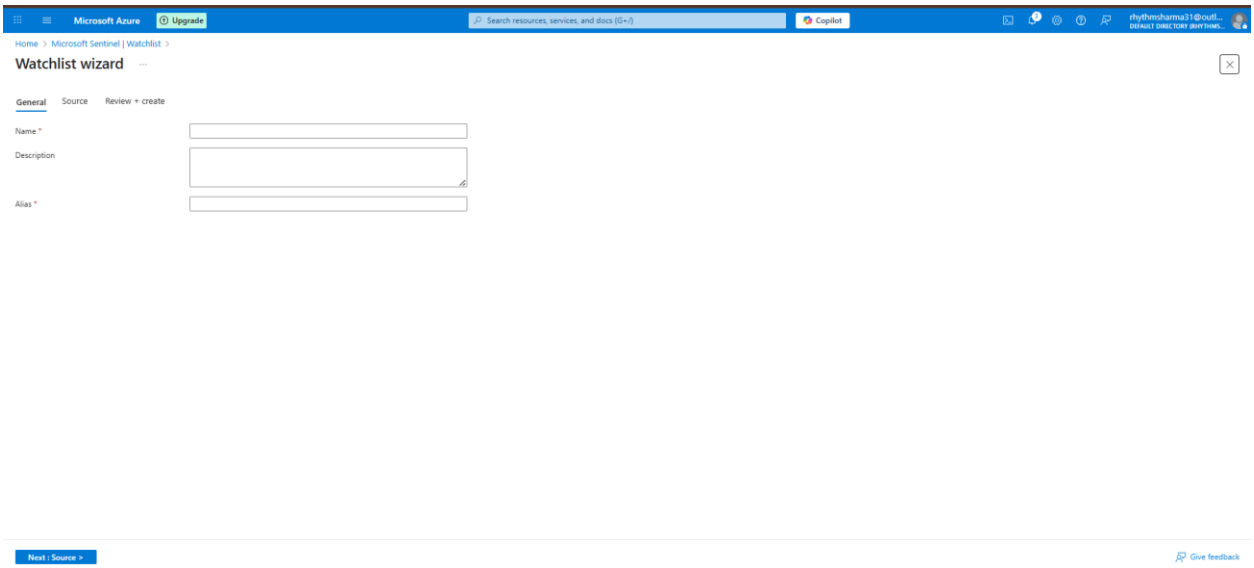
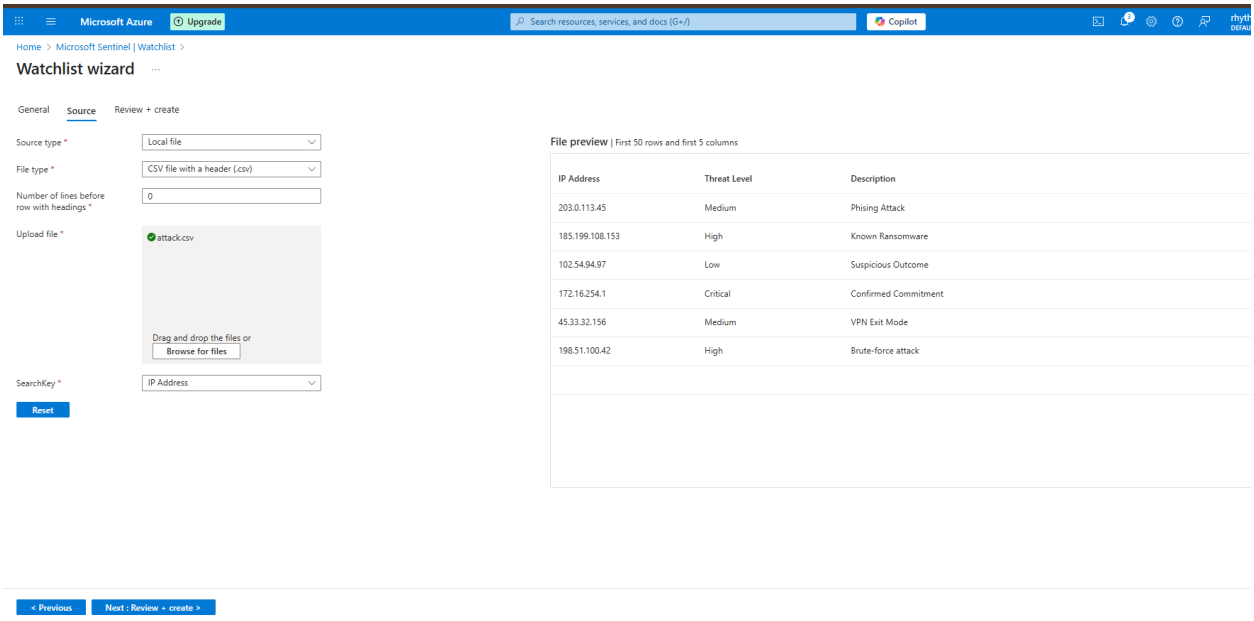
5.1 Watchlist

Microsoft Sentinel watchlist enables the collection of data from external data sources for correlation against the events in your Microsoft Sentinel environment. Once created, leverage watchlists in your search, detection rules, threat hunting, workbooks and response playbooks.

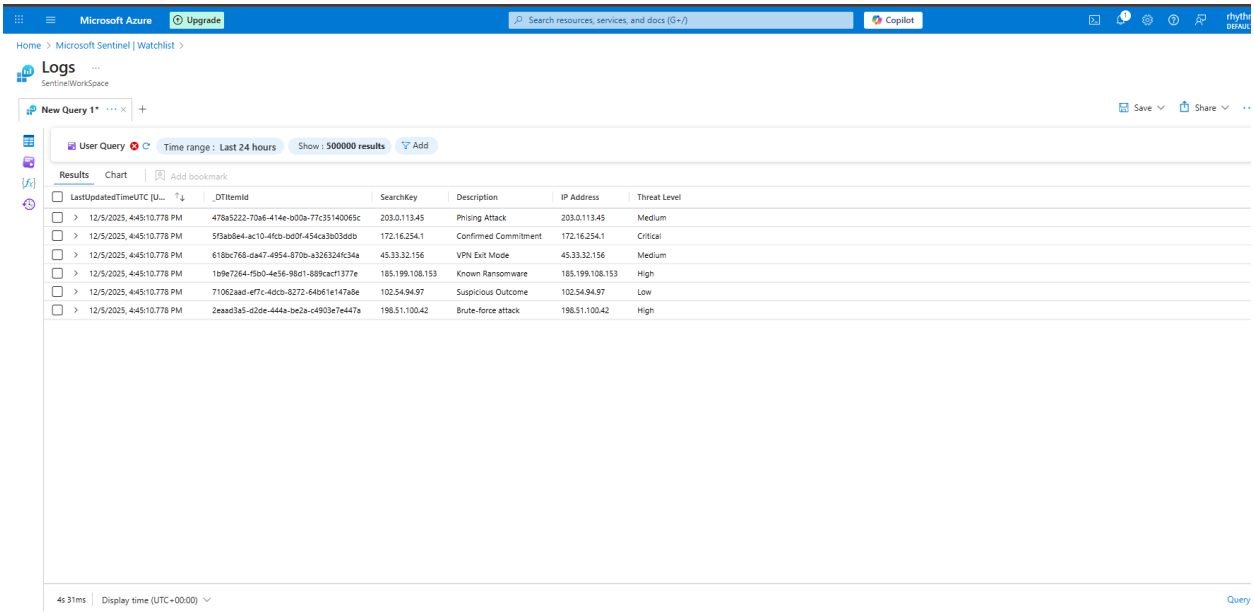
5.1.1 Create Watchlist



5.1.2 Add csv watch list

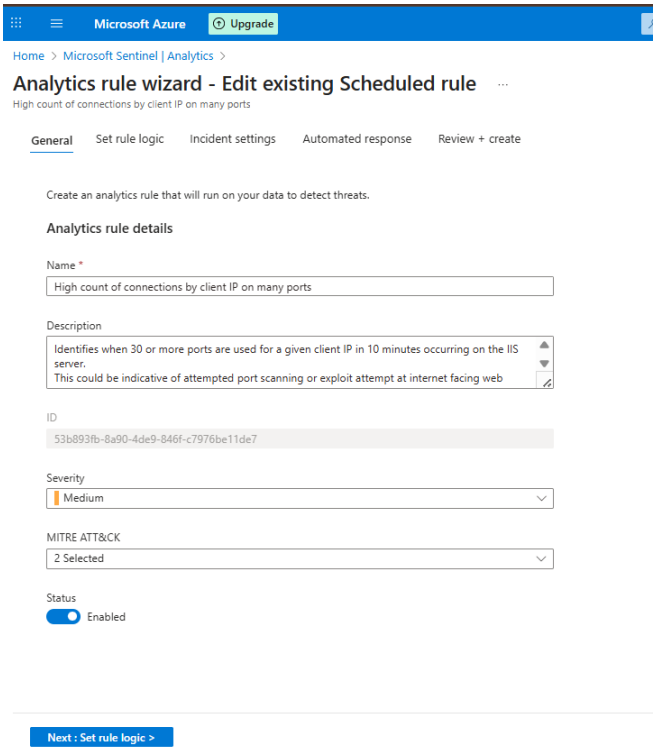


A watchlist is essentially a lookup table. It holds information but doesn't generate alerts or actions on its own.



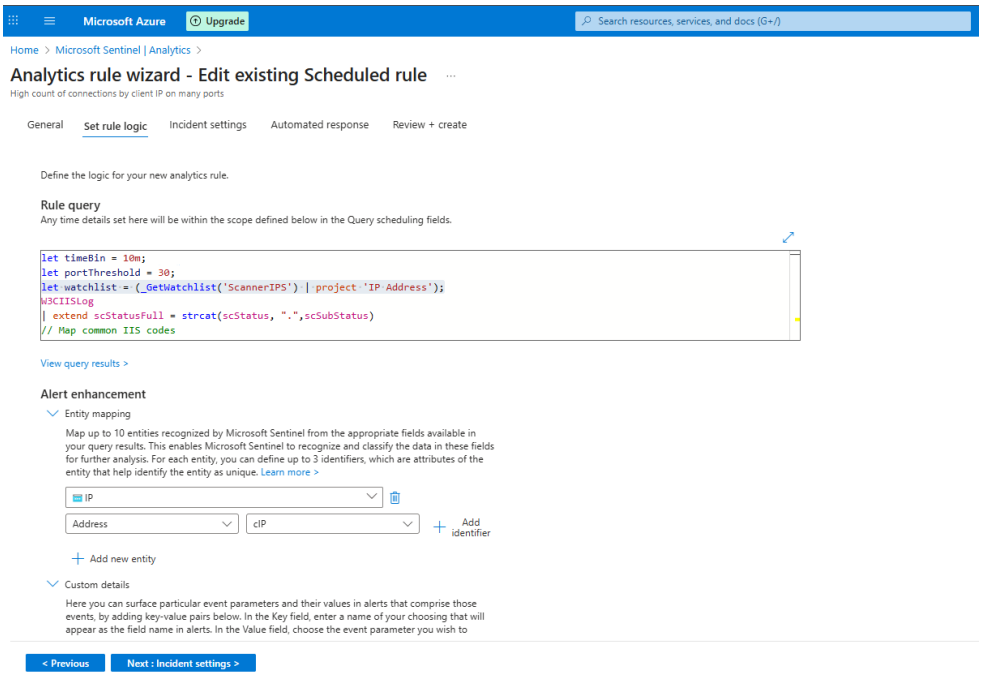
5.1.3 Lets create a analytics rule

An analytics rule is what makes it actionable



Added a line

let watchlist = (_GetWatchlist('ScannerIPS') | project 'IP Address');



5.1.4 Rule saved in analytics