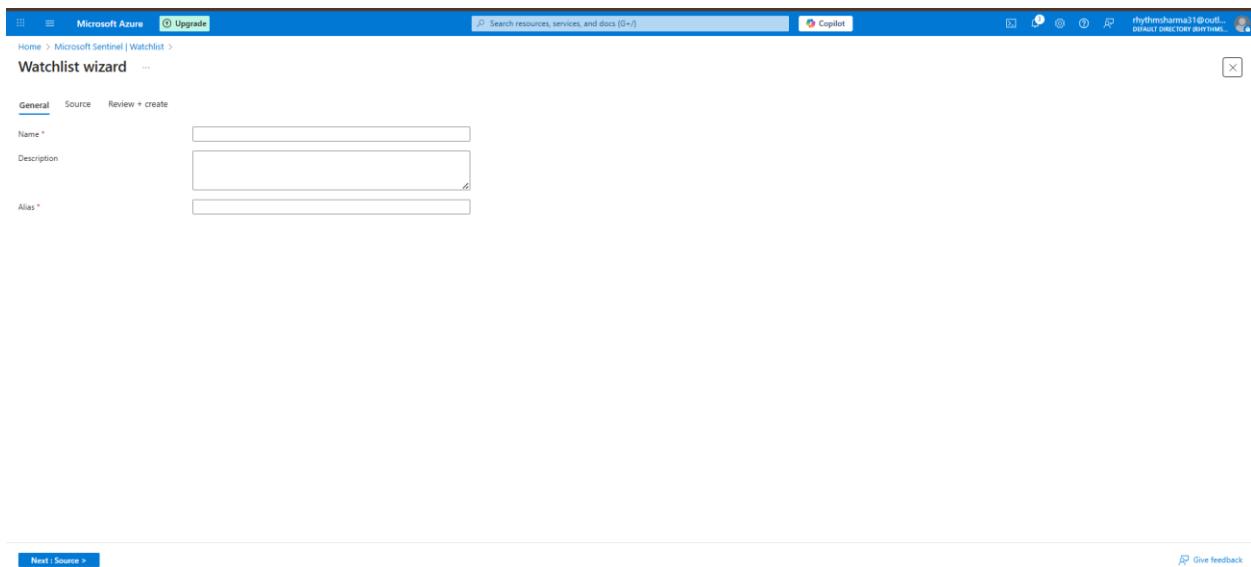


5.1 Watchlist

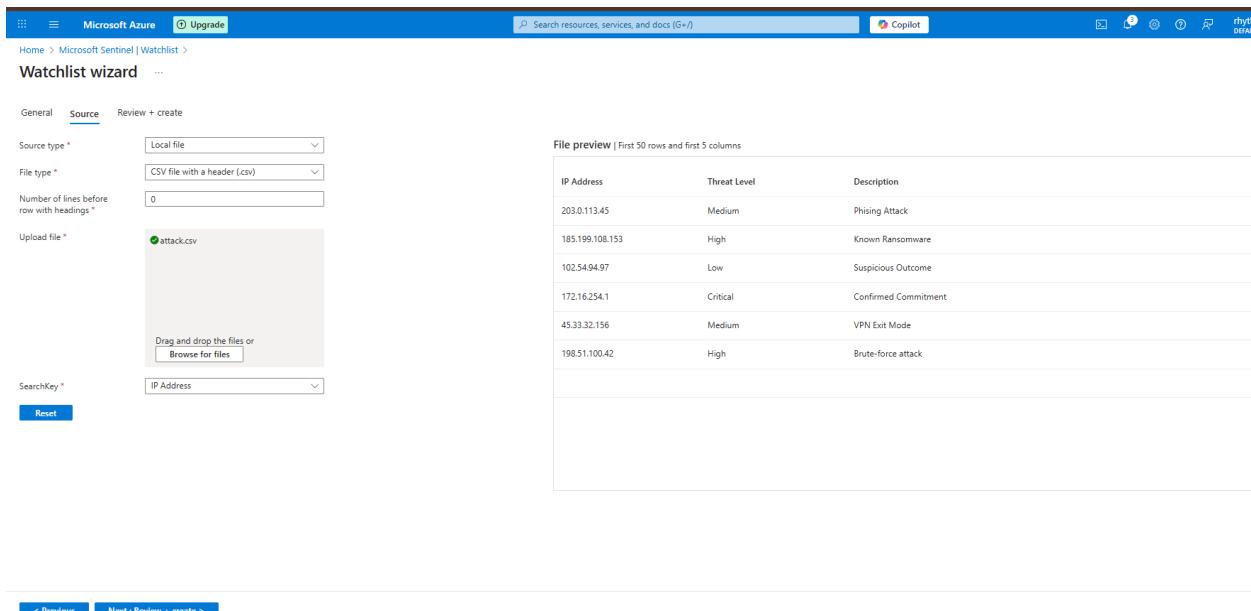
Microsoft Sentinel watchlist enables the collection of data from external data sources for correlation against the events in your Microsoft Sentinel environment. Once created, leverage watchlists in your search, detection rules, threat hunting, workbooks and response playbooks.

5.1.1 Create Watchlist



The screenshot shows the 'Watchlist wizard' interface in the Microsoft Azure portal. The 'General' tab is selected. The 'Name' field contains a redacted value. The 'Description' field contains a redacted value. The 'Alias' field contains a redacted value. Below the fields are 'Next: Source >' and 'Give feedback' buttons.

5.1.2 Add csv watch list



The screenshot shows the 'Watchlist wizard' interface in the Microsoft Azure portal. The 'Source' tab is selected. The 'Source type' dropdown is set to 'Local file'. The 'File type' dropdown is set to 'CSV file with a header (.csv)'. The 'Number of lines before row with headings' input field is set to '0'. A file upload area shows 'attack.csv' uploaded. To the right, a 'File preview' table displays the first 5 rows of the CSV file. The table has columns: IP Address, Threat Level, and Description. The data includes:

IP Address	Threat Level	Description
203.0.113.45	Medium	Phising Attack
185.199.108.153	High	Known Ransomware
102.54.94.97	Low	Suspicious Outcome
172.16.254.1	Critical	Confirmed Commitment
45.33.32.156	Medium	VPN Exit Mode
198.51.100.42	High	Brute-force attack

Below the preview is a 'SearchKey' dropdown and a 'Reset' button. Navigation buttons at the bottom include '< Previous', 'Next: Review + create >', and 'Give feedback'.

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

The screenshot shows the Microsoft Sentinel Log Analytics interface. At the top, there's a navigation bar with 'Microsoft Azure' and 'Upgrade' buttons, a search bar, and a Copilot icon. Below the navigation is a breadcrumb trail: Home > Microsoft Sentinel | Watchlist. The main area is titled 'Logs' and shows a table of search results. The table has columns: LastUpdatedTimeUTC, _ID, SearchKey, Description, IP Address, and Threat Level. The results show various threat events like Phishing Attacks, Confirmed Commitment, and Known Ransomware. At the bottom of the table, there are filters for 'LastUpdatedTimeUTC' and 'SearchKey'. The bottom right corner of the interface has a 'Query' button.

5.1.3 Lets create a analytics rule

An analytics rule is what makes it actionable

The screenshot shows the 'Analytics rule wizard - Edit existing Scheduled rule' page. The title is 'Analytics rule wizard - Edit existing Scheduled rule' with a '...>' button. Below the title, a note says 'High count of connections by client IP on many ports'. There are tabs at the top: General (selected), Set rule logic, Incident settings, Automated response, and Review + create. The General tab contains a description: 'Create an analytics rule that will run on your data to detect threats.' Under 'Analytics rule details', there is a 'Name' field with the value 'High count of connections by client IP on many ports'. A 'Description' field contains the text: 'Identifies when 30 or more ports are used for a given client IP in 10 minutes occurring on the IIS server. This could be indicative of attempted port scanning or exploit attempt at internet facing web'. Below these are fields for 'ID' (53b893fb-8a90-4de9-846f-c7976be11de7), 'Severity' (Medium), 'MITRE ATT&CK' (2 Selected), and 'Status' (Enabled). At the bottom left is a 'Next : Set rule logic >' button.

Added a line

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

The screenshot shows the 'Analytics rule wizard - Edit existing Scheduled rule' interface. At the top, there are tabs: General, Set rule logic (which is selected), Incident settings, Automated response, and Review + create. Below the tabs, a query editor contains the following Power Query M code:

```
let timeBin = 10m;
let portThreshold = 30;
let watchlist = (_GetWatchlist('ScannerIPS') | project 'IP Address');
NSCISLog
| extend scStatusfull = strcat(scStatus, ".",scSubStatus)
// Map common IIS codes
```

Below the code, there's a 'View query results >' link. Under 'Alert enhancement', there's a section for 'Entity mapping' where 'IP' is selected. A dropdown menu shows 'Address' and 'clP' with an 'Add identifier' button. There's also a '+ Add new entity' button. A 'Custom details' section allows adding key-value pairs. At the bottom, there are navigation buttons: '< Previous' and 'Next : Incident settings >'.

5.1.4 Rule saved in analytics

The screenshot shows the Microsoft Sentinel Analytics workspace. On the left, a sidebar lists various sections like General, Threat management, Content management, and Configuration. The main area displays a table of 'Active rules' with the following data:

Severity	Name	Status	Tactics	Techniques	Sub techniques	Source name	Last modified
Medium	High count of connections b...	Enabled	Initial Access	T1190		Standalone	12/5/2023, 11:5...
Medium	multiple failed sign-ins	Enabled	Initial Access			Custom Content	12/4/2023, 21:1...
High	Solorigate Network Beacon	Enabled	Command And Control			Gallery Content	12/4/2023, 12:2...
Medium	Malicious Inbox Rule - custom	Enabled	Persist +1			Custom Content	12/4/2023, 12:2...
Medium	Sign-ins from IPs that attempt...	Enabled	Initial	+1		Gallery Content	12/4/2023, 12:2...

On the right, a 'Notifications' panel shows a message: 'Analytics rule saved' with the note 'Analytics rule "High count of connections by client IP on many ports" saved successfully'. It also includes a 'Dismiss all' button and a link to 'More events in the activity log'.