

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' in the Microsoft Sentinel interface. The 'General' tab is active, showing fields for 'Name *', 'Description', and 'Alias *'. The 'Next: Source >' button is visible at the bottom right.

Microsoft Azure Upgrade

Search resources, services, and docs (G+)

Copilot

Home > Microsoft Sentinel | Watchlist >

Watchlist wizard

General Source Review + create

Name *

Description

Alias *

Next: Source >

Give feedback

5.1.2 Add csv watch list

The screenshot shows the 'Watchlist wizard' in the Microsoft Sentinel interface, now on the 'Source' tab. It displays configuration options for a CSV file source, including 'Source type *', 'File type *', 'Number of lines before row with headings *', 'Upload file *', and 'SearchKey *'. A 'File preview' table is shown on the right, displaying the first 50 rows and first 5 columns of the uploaded CSV file.

Microsoft Azure Upgrade

Search resources, services, and docs (G+)

Copilot

Home > Microsoft Sentinel | Watchlist >

Watchlist wizard

General Source Review + create

Source type *

File type *

Number of lines before row with headings *

Upload file *

SearchKey *

Reset

File preview | First 50 rows and first 5 columns

IP Address	Threat Level	Description
203.0.113.45	Medium	Phishing 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

< Previous

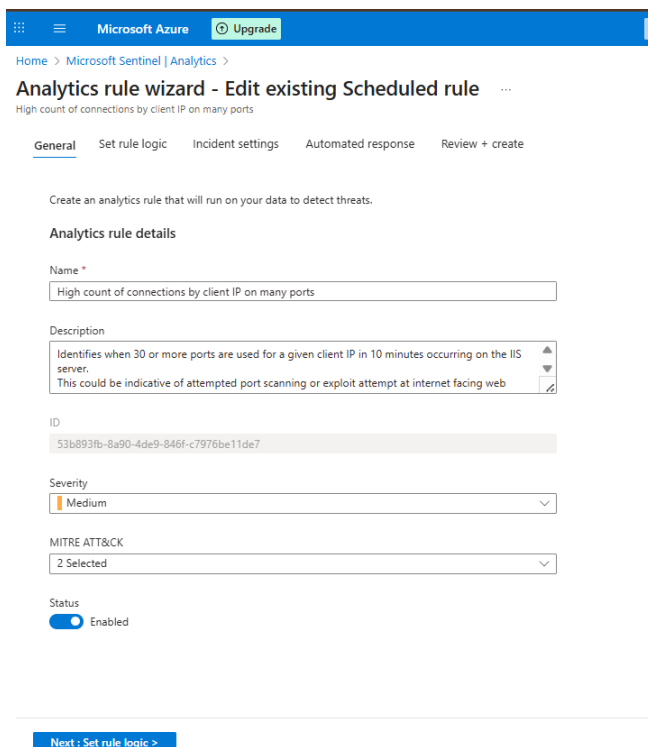
Next: Review + create >

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



The screenshot shows the 'Analytics rule wizard - Edit existing Scheduled rule' page in Microsoft Sentinel. The breadcrumb is 'Home > Microsoft Sentinel | Analytics'. The rule name is 'High count of connections by client IP on many ports'. The description is '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'. The ID is '53b893fb-8a90-4de9-846f-c7976be11de7'. The severity is 'Medium'. The MITRE ATT&CK is '2 Selected'. The status is 'Enabled'. A 'Next: Set rule logic >' button is at the bottom.

Analytics rule details

Name *

High count of connections by client IP on many ports

Description

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

ID

53b893fb-8a90-4de9-846f-c7976be11de7

Severity

Medium

MITRE ATT&CK

2 Selected

Status

Enabled

Next: Set rule logic >

Added a line

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

Microsoft Azure Upgrade Search resources, services, and docs (G+)

Home > Microsoft Sentinel | Analytics >

Analytics rule wizard - Edit existing Scheduled rule

High count of connections by client IP on many ports

General **Set rule logic** Incident settings Automated response Review + create

Define the logic for your new analytics rule.

Rule query
Any time details set here will be within the scope defined below in the Query scheduling fields.

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

[View query results >](#)

Alert enhancement

Entity mapping
Map up to 10 entities recognized by Microsoft Sentinel from the appropriate fields available in your query results. This enables Microsoft Sentinel to recognize and classify the data in these fields for further analysis. For each entity, you can define up to 3 identifiers, which are attributes of the entity that help identify the entity as unique. [Learn more >](#)

IP Address cIP + Add identifier

+ Add new entity

Custom details
Here you can surface particular event parameters and their values in alerts that comprise those events, by adding key-value pairs below. In the Key field, enter a name of your choosing that will appear as the field name in alerts. In the Value field, choose the event parameter you wish to

< Previous Next: Incident settings >

5.1.4 Rule saved in analytics

Microsoft Azure Upgrade Search resources, services, and docs (G+)

Home > Microsoft Sentinel

Microsoft Sentinel | Analytics

Search Create Refresh Analytics workbooks Rule runs (Preview) Enable Disable Delete Import Export Columns Guides & Feedback

5 Active rules More content at Content hub Rules by severity: High (1) Medium (4) Low (0) Informational (0) LEARN MORE About analytics rules

Active rules Rule templates Anomalies

Search by ID, name, tactic or technique Add filter

Severity	Name	Rule L...	Status	Tactics	Techniques	Sub techniques	Source name	Last modified
Medium	High count of connections b...	S...	Enabled	Initial Access	T1190		Standalone	12/5/2025, 11:5...
Medium	multiple failed sign-ins	S...	Enabled	Initial Access			Custom Content	12/4/2025, 2:11...
High	Solorigate Network Beacon	S...	Enabled	Command An			Gallery Content	12/4/2025, 12:2...
Medium	Malicious Inbox Rule - custom	S...	Enabled	Persist +1			Custom Content	12/4/2025, 12:2...
Medium	Sign-ins from IPs that attempt...	S...	Enabled	Initial +1			Gallery Content	12/4/2025, 12:2...

Notifications

More events in the activity log Dismiss all

Analytics rule saved
Analytics rule 'High count of connections by client IP on many ports' saved successfully
a few seconds

< Previous Page 1 of 1 Next > Showing 1 to 5 of 5 results