

Microsoft Azure | Upgrade | Search resources, services, and docs (G+I) | Copilot | rhythmsharma31@outlook.com | Connect Defender Threat Intel

Microsoft Defender Threat Intelligence

Connected Status: Microsoft Provider | 3 Minutes Ago | Last Log Received: 12/5/2025, 11:53:52 AM

Content source: Threat Intelligence (NEW) | Version: 1.0.0 | Author: Microsoft | Supported by: Microsoft Corporation | Email

Related content: 0 Workbooks | 4 Queries | 51 Analytics rules templates

Data received: 140K | 105K | 70K | 35K | 0 | Go to log analytics

Data types: ThreatIntelligence | ThreatIntIndicators | ThreatIntObjects

Prerequisites

To integrate with Microsoft Defender Threat Intelligence make sure you have:

- ✓ **Workspaces:** read and write permissions.

Configuration

Use this data connector to import Indicators of Compromise (IOCs) from Microsoft Defender Threat Intelligence (MDTI) into Microsoft Sentinel.

Data last received on: --

Recommended log sources for matching:

- Amazon Web Services
- Microsoft Entra ID
- Azure Activity
- VPN
- Azure Firewall
- Barracuda Web Application Firewall
- Azure Web Application Firewall (WAF)
- Windows DNS via Legacy Agent
- Microsoft 365 (formerly, Office 365)

Disconnect

Explore TI menu

Microsoft Azure | Upgrade | Search resources, services, and docs (G+I) | Copilot | rhythmsharma31@outlook.com | Connect Defender Threat Intel

Microsoft Sentinel | Threat intelligence

Selected workspace: sentinelnewworkspace

Refresh | New | Add tags | Delete | Columns | Import | Export (Preview) | Ingestion rules | Threat intelligence workbook | Guides & Feedback

Filters

Indicators (99,353)	Attack patterns (0)	Identities (1)	Threat actors (0)	Relationships (0)
<input type="checkbox"/> Values				
<input type="checkbox"/> 219.152.170.58		Microsoft Identified IOC	Network traffi	Microsoft Defender Thre...
<input type="checkbox"/> 118.193.45.235		Microsoft Identified IOC	Network traffi	Microsoft Defender Thre...
<input type="checkbox"/> 91.196.152.99		Microsoft Identified IOC	Network traffi	Microsoft Defender Thre...
<input type="checkbox"/> 139.19.117.129		Microsoft Identified IOC	Network traffi	Microsoft Defender Thre...
<input type="checkbox"/> 167.94.138.327		Microsoft Identified IOC	Network traffi	Microsoft Defender Thre...
<input type="checkbox"/> 3.80.46.54		Microsoft Identified IOC	Network traffi	Microsoft Defender Thre...
<input type="checkbox"/> 112.81.106.222		Microsoft Identified IOC	Network traffi	Microsoft Defender Thre...
<input type="checkbox"/> 101.36.123.67		Microsoft Identified IOC	Network traffi	Microsoft Defender Thre...
<input type="checkbox"/> 173.175.136.75		Microsoft Identified IOC	Network traffi	Microsoft Defender Thre...
<input type="checkbox"/> 140.245.70.130		Microsoft Identified IOC	Network traffi	Microsoft Defender Thre...
<input type="checkbox"/> 196.18.230.18		Microsoft Identified IOC	Network traffi	Microsoft Defender Thre...
<input type="checkbox"/> 187.210.77.100		Microsoft Identified IOC	Network traffi	Microsoft Defender Thre...
<input type="checkbox"/> 112.199.164.41		Microsoft Identified IOC	Network traffi	Microsoft Defender Thre...
<input type="checkbox"/> 185.142.236.41		Microsoft Identified IOC	Network traffi	Microsoft Defender Thre...

1 - 100 | Previous | Next

New TI object

Object type: Indicator

Pattern: Pattern builder | Free text

URL: URL value *

Valid from: 12/5/2025 | Valid until: 12/03/00 PM

Source: No conflict found.

Add | Cancel | Add and duplicate

I can add my IoCs for threat intelligence

Microsoft Azure

Upgrade

Search resources, services, and docs (S+)

Copilot

rythmsharma31@outlook.com

Home > Microsoft Sentinel

Microsoft Sentinel | Threat intelligence

Selected workspace: 'sentinelworkspace'

Search

Refresh + New + Add tags Delete Columns Import Export (Preview) Ingestion rules Threat intelligence workbook Guides & Feedback

General

Overview

Logs

Guides

Search

Threat management

Incidents

Workbooks

Hunting

Notebooks

Entity behavior

Threat intelligence

MITRE ATT&CK (Preview)

SOC optimization

Content management

Content hub

Repositories

Community

Configuration

Workspace manager (Preview)

Data connectors

Analytics

Filters

Indicators (99,369)

Attack patterns (0)

Identities (1)

Threat actors (0)

Relationships (0)

Values	Name	Types	Source	Confidence	Alerts	Tags	Valid from	Valid until	Exports	
<input type="checkbox"/>	187.232.26.62	Microsoft Identified IOC	Network traffic	Microsoft Defender Threat ...	100	0	honeypot +6	12/5/2023, 12:04:46 ...	12/5/2023, 5:04:45
<input checked="" type="checkbox"/>	hacker.ca	MaliciousURL	URL	Microsoft Sentinel	--	0	--	12/5/2023, 12:03:00 ...	12/4/2026, 12:00:00
<input type="checkbox"/>	162.142.125.208	Microsoft Identified IOC	Network traffic	Microsoft Defender Threat ...	100	0	honeypot +6	12/5/2023, 12:04:21 ...	12/5/2023, 5:04:19
<input type="checkbox"/>	167.94.138.178	Microsoft Identified IOC	Network traffic	Microsoft Defender Threat ...	100	0	honeypot +6	12/5/2023, 12:02:21 ...	12/5/2023, 5:02:19
<input type="checkbox"/>	138.219.173.168	Microsoft Identified IOC	Network traffic	Microsoft Defender Threat ...	100	0	honeypot +6	12/5/2023, 12:04:31 ...	12/5/2023, 5:04:26
<input type="checkbox"/>	187.17.163.7	Microsoft Identified IOC	Network traffic	Microsoft Defender Threat ...	100	0	honeypot +6	12/5/2023, 12:04:01 ...	12/5/2023, 5:03:58
<input type="checkbox"/>	54.91.75.17	Microsoft Identified IOC	Network traffic	Microsoft Defender Threat ...	100	0	honeypot +6	12/5/2023, 12:03:44 ...	12/5/2023, 5:03:36
<input type="checkbox"/>	65.49.20.68	Microsoft Identified IOC	Network traffic	Microsoft Defender Threat ...	100	0	honeypot +6	12/5/2023, 12:03:35 ...	12/5/2023, 5:03:34
<input type="checkbox"/>	108.190.104.183	Microsoft Identified IOC	Network traffic	Microsoft Defender Threat ...	100	0	honeypot +6	12/5/2023, 12:03:30 ...	12/5/2023, 5:03:25
<input type="checkbox"/>	85.133.193.72	Microsoft Identified IOC	Network traffic	Microsoft Defender Threat ...	100	0	honeypot +6	12/5/2023, 12:04:21 ...	12/5/2023, 5:04:16
<input type="checkbox"/>	202.75.28.141	Microsoft Identified IOC	Network traffic	Microsoft Defender Threat ...	100	0	honeypot +6	12/5/2023, 12:04:19 ...	12/5/2023, 5:04:15
<input type="checkbox"/>	189.231.254.145	Microsoft Identified IOC	Network traffic	Microsoft Defender Threat ...	100	0	honeypot +6	12/5/2023, 12:02:59 ...	12/5/2023, 5:02:51
<input type="checkbox"/>	91.231.89.5	Microsoft Identified IOC	Network traffic	Microsoft Defender Threat ...	100	0	honeypot +6	12/5/2023, 12:03:55 ...	12/5/2023, 5:03:54
<input type="checkbox"/>	64.62.156.66	Microsoft Identified IOC	Network traffic	Microsoft Defender Threat ...	100	0	honeypot +6	12/5/2023, 12:02:44 ...	12/5/2023, 5:02:42
<input type="checkbox"/>	87.251.67.57	Microsoft Identified IOC	Network traffic	Microsoft Defender Threat ...	100	0	honeypot +6	12/5/2023, 12:03:56 ...	12/5/2023, 5:03:55

< Previous 1 - 100 Next >

Add or remove favorites by pressing Ctrl+click on it

Microsoft Azure

Upgrade

Search resources, services, and docs (S+)

Copilot

rythmsharma31@outlook.com

Home > Microsoft Sentinel

Microsoft Sentinel | Workbooks

Selected workspace: 'sentinelworkspace'

Search

Refresh + Add Workbook Guides & Feedback

General

Overview

Logs

Guides

Search

Threat management

Incidents

Workbooks

Hunting

Notebooks

Entity behavior

Threat intelligence

MITRE ATT&CK (Preview)

SOC optimization

Content management

Content hub

Repositories

Community

Configuration

Workspace manager (Preview)

Data connectors

Analytics

1 My workbooks

6 Templates

0 Updates

More content at Content hub

My workbooks

Templates

Search

Add filter

Name	Status	Source name
Azure Activity	--	Azure Activity
Azure Service Health Workbook	--	Azure Activity
Microsoft Entra ID Audit logs	--	Microsoft Entra ID
Microsoft Entra ID Sign-in logs	--	Microsoft Entra ID
Threat Intelligence	--	Microsoft Defender Threat Intelligence
Threat Intelligence	--	Threat Intelligence (NEW)

Threat Intelligence

Status Not saved

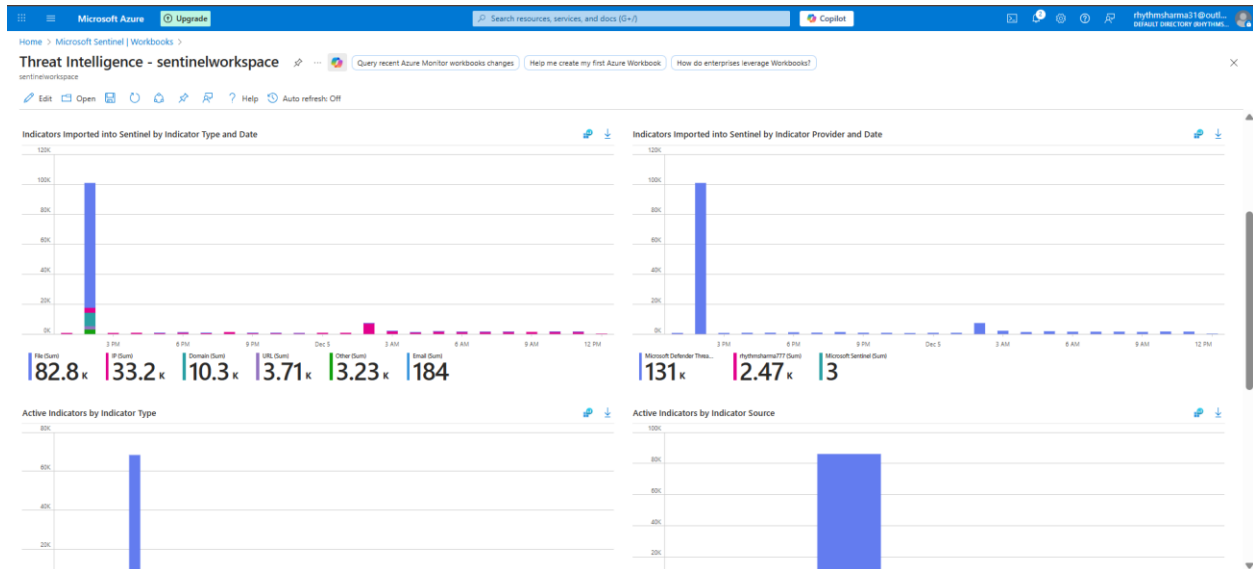
Description Gain insights into threat indicators ingestion and search for indicators at scale across Microsoft 1st Party, 3rd Party, On-Premises, Hybrid, and Multi-Cloud Workloads. Indicators Search facilitates a simple interface for finding IP, File, Hash, Sender and more across your data. Seamless pivots to correlate indicators with Microsoft Sentinel incidents to make your threat intelligence actionable.

Content source Threat Intelligence (NEW) Template version 1.0.0

Author Microsoft Supported by Microsoft Corporation | Email

View Template Save

Add or remove favorites by pressing Ctrl+click on it



We can edit a query according to our need

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

Home > Microsoft Sentinel | Workbooks >

Threat Intelligence - sentinelworkspace

sentinelworkspace

Query recent Azure Monitor workbooks changes | Help me create my first Azure Workbook | How do enterprises leverage Workbooks?

Done Editing | Open | Auto refresh Off

Editing query item: query - 9

Settings | Advanced Settings | Style | Advanced Editor

Run Query | Samples | Data source: Logs (Analytics) | Resource type: Log Analytics | Log Analytics workspace: sentinelworkspace | Time Range: Last 24 hours | Visualization: Set by query | Size: Medium

Log Analytics workspace Logs (Analytics) Query

No query was specified.