

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

Home > Microsoft Sentinel | Data connectors >

Microsoft Defender Threat Intelligence

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 November 30 December 2 December 4

Go to log analytics

ThreatIntelIndicators 131K ThreatIntelObjects 0

Data types ThreatIntelIndicators 12/5/2025, 11:53:52 AM ThreatIntelObjects --

Prerequisites

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

- ✓ Workspace: 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
- Office Activity
- VPN
- Azure Firewall
- Baracuda Web Application Firewall
- Microsoft Configuration Manager (MCM)
- Windows DNS via Legacy Agent
- Microsoft 365 (formerly, Office 365)

Disconnect

Explore TI menu

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

Home > Microsoft Sentinel

Microsoft Sentinel | Threat intelligence

Selected workspace: sentinelworkspace

Search

General

- Overview
- Logs
- Guides
- Search

Treat 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

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) | | | | |
|---------------------|--------------------------|-----------------|----------------------------|-------------------|--------|----------|------------|---------------|
| Values | Name | Types | Source | Confidence | Alerts | Tags | Valid from | |
| 219.152.170.58 | Microsoft Identified IOC | Network traffic | Microsoft Defender Thre... | 100 | 0 | honeypot | +6 | 12/5/2025, 12 |
| 118.193.45.235 | Microsoft Identified IOC | Network traffic | Microsoft Defender Thre... | 100 | 0 | honeypot | +6 | 12/5/2025, 11 |
| 91.196.152.99 | Microsoft Identified IOC | Network traffic | Microsoft Defender Thre... | 100 | 0 | honeypot | +6 | 12/5/2025, 11 |
| 139.18.117.129 | Microsoft Identified IOC | Network traffic | Microsoft Defender Thre... | 100 | 0 | honeypot | +6 | 12/5/2025, 11 |
| 167.94.138.127 | Microsoft Identified IOC | Network traffic | Microsoft Defender Thre... | 100 | 0 | honeypot | +6 | 12/5/2025, 12 |
| 3.80.46.54 | Microsoft Identified IOC | Network traffic | Microsoft Defender Thre... | 100 | 0 | honeypot | +6 | 12/5/2025, 12 |
| 112.81.106.222 | Microsoft Identified IOC | Network traffic | Microsoft Defender Thre... | 100 | 0 | honeypot | +6 | 12/5/2025, 12 |
| 101.36.123.67 | Microsoft Identified IOC | Network traffic | Microsoft Defender Thre... | 100 | 0 | honeypot | +6 | 12/5/2025, 11 |
| 173.175.136.75 | Microsoft Identified IOC | Network traffic | Microsoft Defender Thre... | 100 | 0 | honeypot | +6 | 12/5/2025, 11 |
| 140.245.70.130 | Microsoft Identified IOC | Network traffic | Microsoft Defender Thre... | 100 | 0 | honeypot | +6 | 12/5/2025, 12 |
| 196.18.230.18 | Microsoft Identified IOC | Network traffic | Microsoft Defender Thre... | 100 | 0 | honeypot | +6 | 12/5/2025, 12 |
| 187.210.77.100 | Microsoft Identified IOC | Network traffic | Microsoft Defender Thre... | 100 | 0 | honeypot | +6 | 12/5/2025, 11 |
| 112.199.164.41 | Microsoft Identified IOC | Network traffic | Microsoft Defender Thre... | 100 | 0 | honeypot | +6 | 12/5/2025, 11 |
| 185.142.236.41 | Microsoft Identified IOC | Network traffic | Microsoft Defender Thre... | 100 | 0 | honeypot | +6 | 12/5/2025, 11 |

< Previous 1 - 100 Next >

New TI object

Object type * Indicator

Pattern *

Pattern builder Free text

URL URL value * This field is required

+ New observable

Unvalue "] Name

Indicator types

Kill chains + Add kill chain

Valid from * 12/5/2025 12:03:00 PM

Valid until MM/DD/YYYY hh:mm:ss aa

Source

No conflict found.

Add Cancel Add and duplicate

I can add my IOCs for threat intelligence

Microsoft Sentinel | Threat intelligence

Selected workspace: 'sentinelworkspace'

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

Indicators (99,369)

| Values | Name | Types | Source | Confidence | Alerts | Tags | Valid from | Valid until | Exports |
|-----------------|--------------------------|-----------------|-------------------------------|------------|--------|-------------|-------------------------|-------------------------|---------|
| 187.232.26.62 | Microsoft Identified IOC | Network traffic | Microsoft Defender Threat ... | 100 | 0 | honeypot +6 | 12/5/2025, 12:04:46 ... | 12/5/2025, 5:04:45 ... | ... |
| hacker.ca | MaliciousURL | URL | Microsoft Sentinel | -- | 0 | -- | 12/5/2025, 12:03:00 ... | 12/4/2026, 12:00:00 ... | ... |
| 162.142.125.208 | Microsoft Identified IOC | Network traffic | Microsoft Defender Threat ... | 100 | 0 | honeypot +6 | 12/5/2025, 12:04:21 ... | 12/5/2025, 5:04:19 ... | ... |
| 167.94.138.178 | Microsoft Identified IOC | Network traffic | Microsoft Defender Threat ... | 100 | 0 | honeypot +6 | 12/5/2025, 12:02:21 ... | 12/5/2025, 5:02:19 ... | ... |
| 138.219.173.168 | Microsoft Identified IOC | Network traffic | Microsoft Defender Threat ... | 100 | 0 | honeypot +6 | 12/5/2025, 12:04:31 ... | 12/5/2025, 5:04:26 ... | ... |
| 187.17.163.7 | Microsoft Identified IOC | Network traffic | Microsoft Defender Threat ... | 100 | 0 | honeypot +6 | 12/5/2025, 12:04:01 ... | 12/5/2025, 5:03:58 ... | ... |
| 54.91.75.17 | Microsoft Identified IOC | Network traffic | Microsoft Defender Threat ... | 100 | 0 | honeypot +6 | 12/5/2025, 12:03:44 ... | 12/5/2025, 5:03:36 ... | ... |
| 65.49.20.68 | Microsoft Identified IOC | Network traffic | Microsoft Defender Threat ... | 100 | 0 | honeypot +6 | 12/5/2025, 12:03:35 ... | 12/5/2025, 5:03:34 ... | ... |
| 108.190.104.183 | Microsoft Identified IOC | Network traffic | Microsoft Defender Threat ... | 100 | 0 | honeypot +6 | 12/5/2025, 12:03:30 ... | 12/5/2025, 5:03:25 ... | ... |
| 85.133.192.72 | Microsoft Identified IOC | Network traffic | Microsoft Defender Threat ... | 100 | 0 | honeypot +6 | 12/5/2025, 12:04:21 ... | 12/5/2025, 5:04:16 ... | ... |
| 202.75.28.141 | Microsoft Identified IOC | Network traffic | Microsoft Defender Threat ... | 100 | 0 | honeypot +6 | 12/5/2025, 12:04:19 ... | 12/5/2025, 5:04:15 ... | ... |
| 189.231.254.145 | Microsoft Identified IOC | Network traffic | Microsoft Defender Threat ... | 100 | 0 | honeypot +6 | 12/5/2025, 12:02:59 ... | 12/5/2025, 5:02:51 ... | ... |
| 91.231.89.5 | Microsoft Identified IOC | Network traffic | Microsoft Defender Threat ... | 100 | 0 | honeypot +6 | 12/5/2025, 12:03:55 ... | 12/5/2025, 5:03:54 ... | ... |
| 64.62.156.66 | Microsoft Identified IOC | Network traffic | Microsoft Defender Threat ... | 100 | 0 | honeypot +6 | 12/5/2025, 12:02:44 ... | 12/5/2025, 5:02:42 ... | ... |
| 87.251.67.57 | Microsoft Identified IOC | Network traffic | Microsoft Defender Threat ... | 100 | 0 | honeypot +6 | 12/5/2025, 12:03:56 ... | 12/5/2025, 5:03:55 ... | ... |

< Previous 1 - 100 Next >

Microsoft Sentinel | Workbooks

Selected workspace: 'sentinelworkspace'

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

My workbooks

| 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) |

Templates

| Name | Updates |
|--------------|---------|
| My workbooks | 0 |
| Templates | 6 |

More content at Content hub

Threat Intelligence

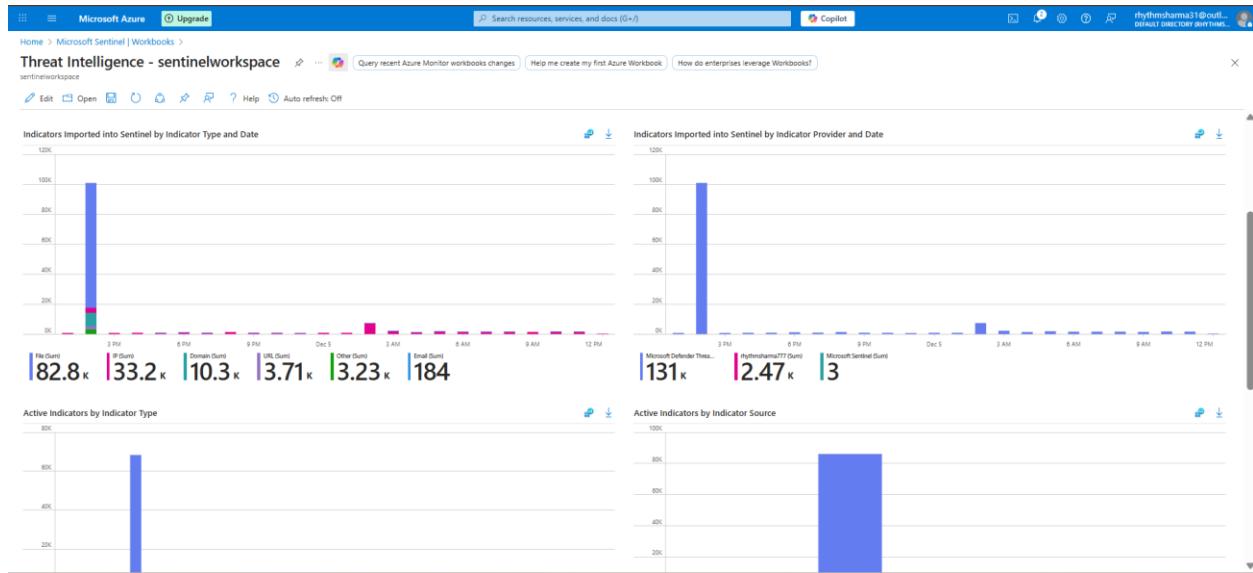
Status: Not saved

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) Version: 1.0.0

Author: Microsoft Supported by: Microsoft Corporation | Email

[View Template](#) [Save](#)



We can edit a query according to our need

Editing query item: query - 9

Settings Advanced Settings Style Advanced Editor

Data source: Log Analytics workspace: sentinelworkspace Resource type: Log Analytics Log Analytics workspace: sentinelworkspace Time Range: Last 24 hours Visualization: Size: Medium

Run Query Samples Logs (Analytics) Log Analytics Query

No query was specified.