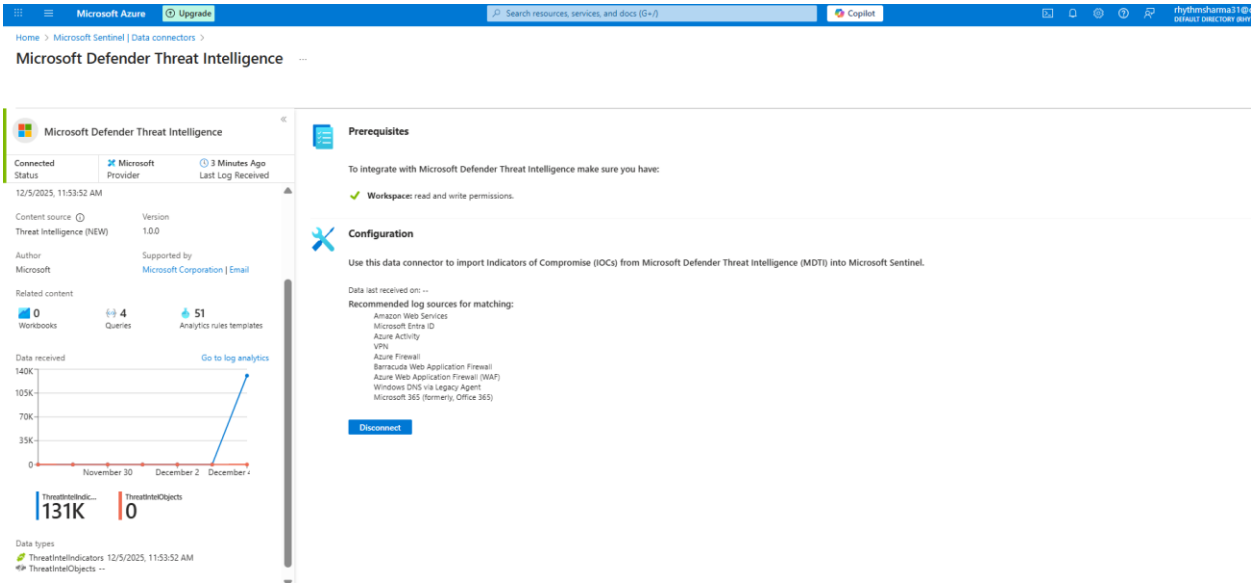
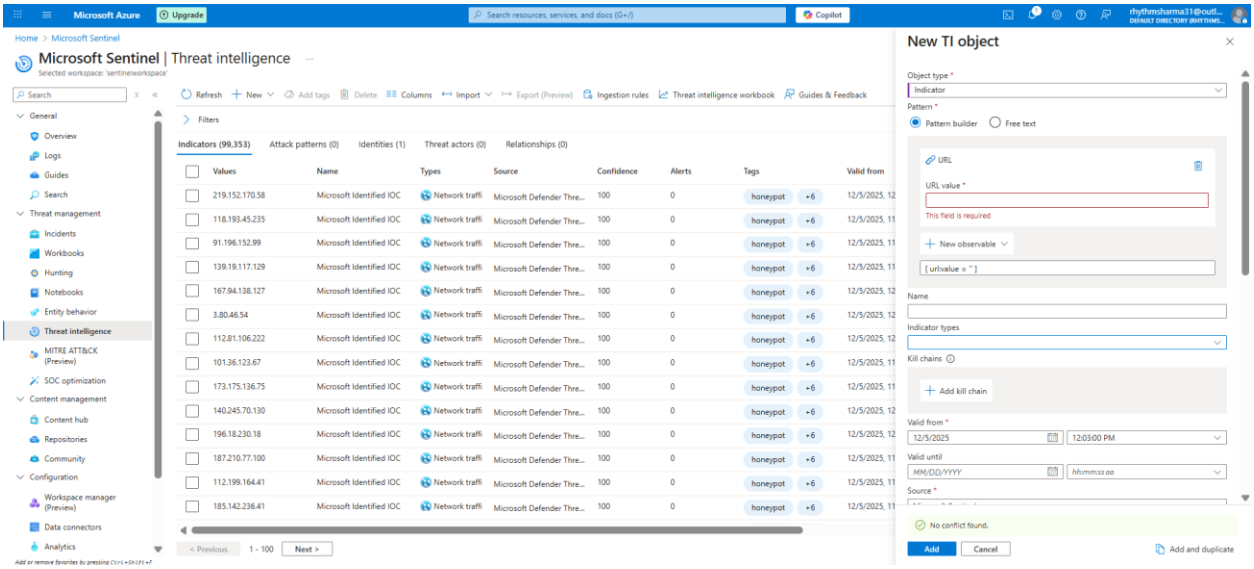
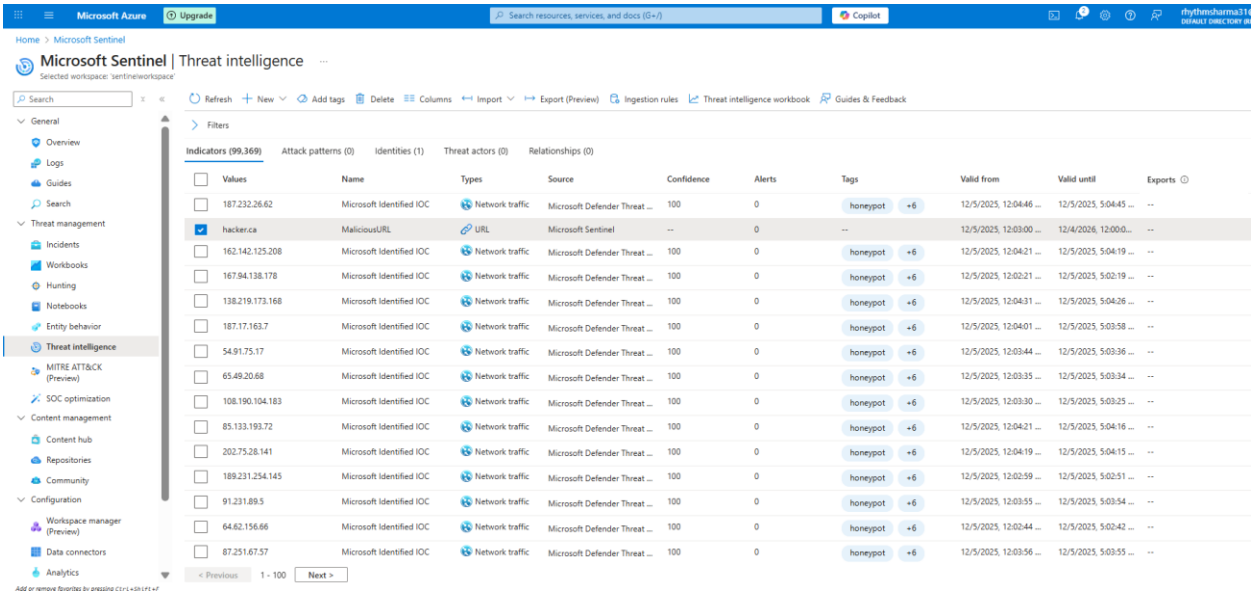
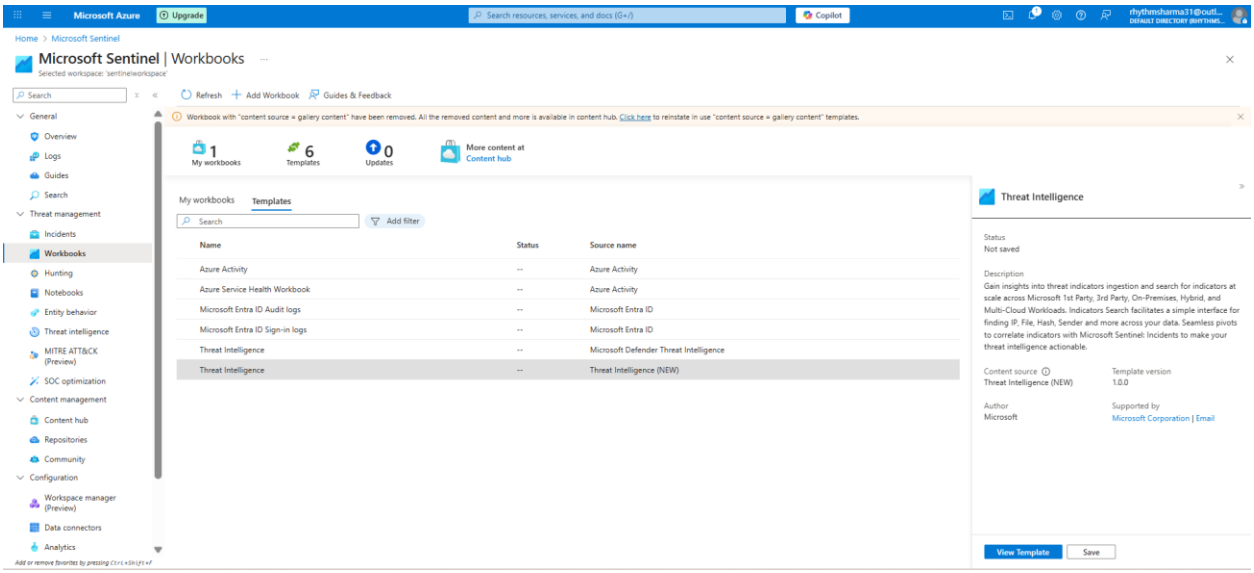


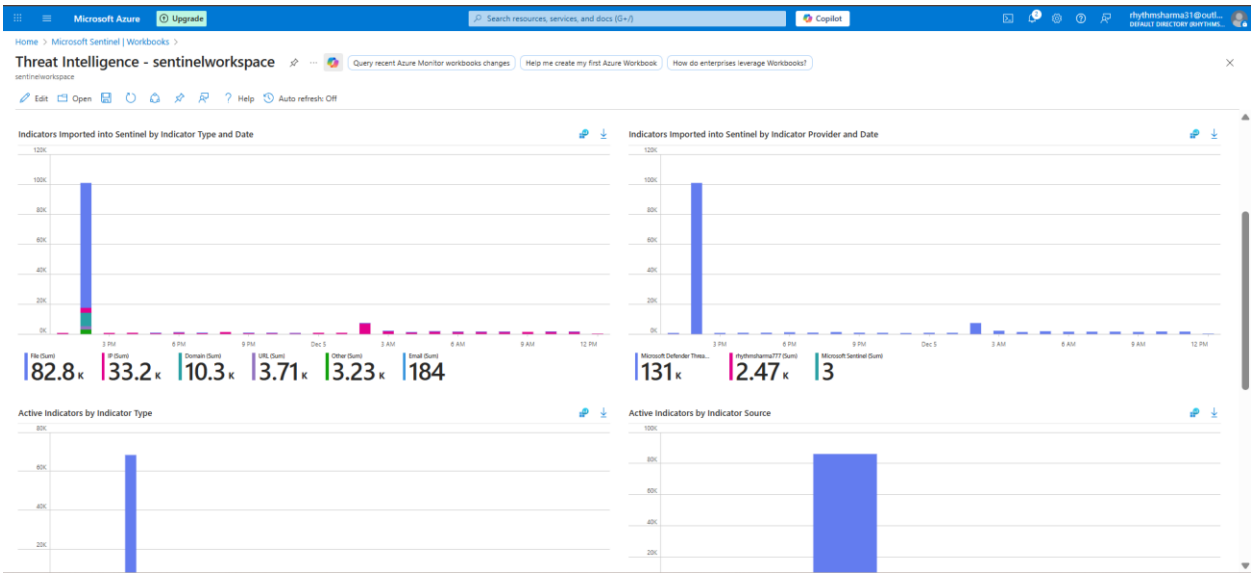
Explore TI menu



I can add my IoCs for threat intelligence


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft Sentinel
Microsoft Sentinel | Threat intelligence
Selected workspace: 'sentinelworkspace'
Refresh
New
Add tags
Delete
Columns
Import
Export (Preview)
Ingestion rules
Threat intelligence workbook
Guides & Feedback
Filters
Indicators (99,369)
Attack patterns (0)
Identities (1)
Threat actors (0)
Relationships (0)
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
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, 12:00:0...
162.142.125.208
167.94.138.178
138.219.173.168
187.17.163.7
54.91.75.17
65.49.20.68
108.190.104.183
85.133.193.72
202.75.28.141
189.231.254.145
91.231.89.5
64.62.156.66
87.251.67.57
< Previous
1 - 100
Next >


Microsoft Azure
Upgrade
Copilot
Home > Microsoft Sentinel
Microsoft Sentinel | Workbooks
Selected workspace: 'sentinelworkspace'
Refresh
Add Workbook
Guides & Feedback
Workbook with "content source = gallery content" have been removed. All the removed content and more is available in content hub. Click here to reinstate in use "content source = gallery content" templates.
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 Service Health Workbook
Microsoft Entra ID Audit logs
Microsoft Entra ID Sign-in logs
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



We can edit a query according to our need