CYBERSECURITY: SIEM

Sentinel Configuration,

14 SEPTEMBER 2025

Michael Musoke

Contents

Introduction

In this Security Operations Centre (SOC) simulation, a Honeynet environment is deployed in an Azure subscription and using a Windows 10 virtual machine exposed to the internet. The security event logs from the system are ingested into Microsoft Sentinel for monitoring and analysis. During the simulation, a brute force attack is detected, and an incident is manually generated, assigned to a SOC analyst, and investigated.

Topology

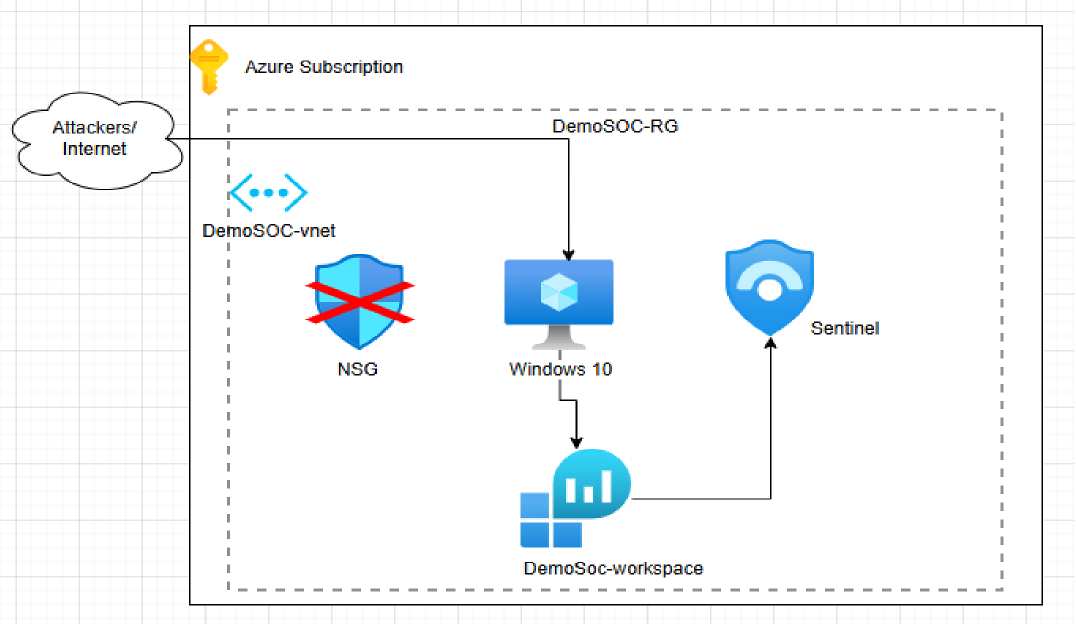


Fig 1

Configuration

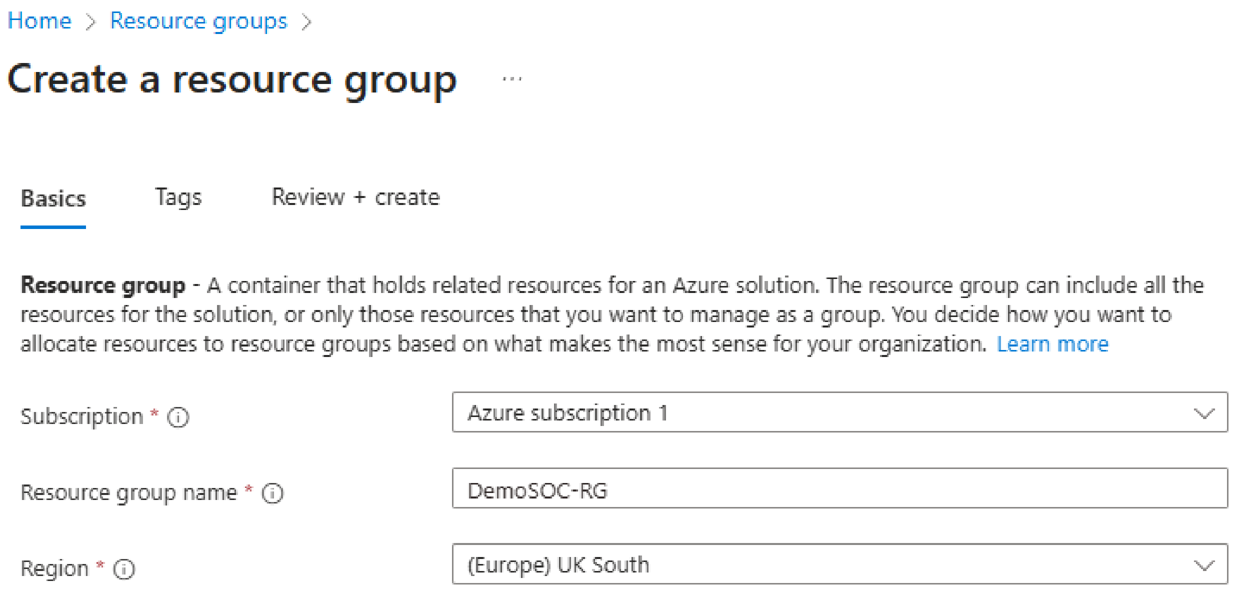
What is Sentinel?

Microsoft Sentinel is a cloud-native Security Information Event Management (SIEM) system. It collects, normalises, and analyses security logs/events from across your environment (On-prem, Cloud, third party)

Sentinel is also a Security Orchestration Automation and Response (SOAR). It automates responses with playbooks, so incidents can be contained or remediated quickly without manual effort.

Create a Resource group (RG)

In an Azure account under and subscription, create a resource group. A resource group is a logical container that holds related Azure resources.



Home > Resource groups >

Create a resource group ···

Basics   Tags   Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. Learn more

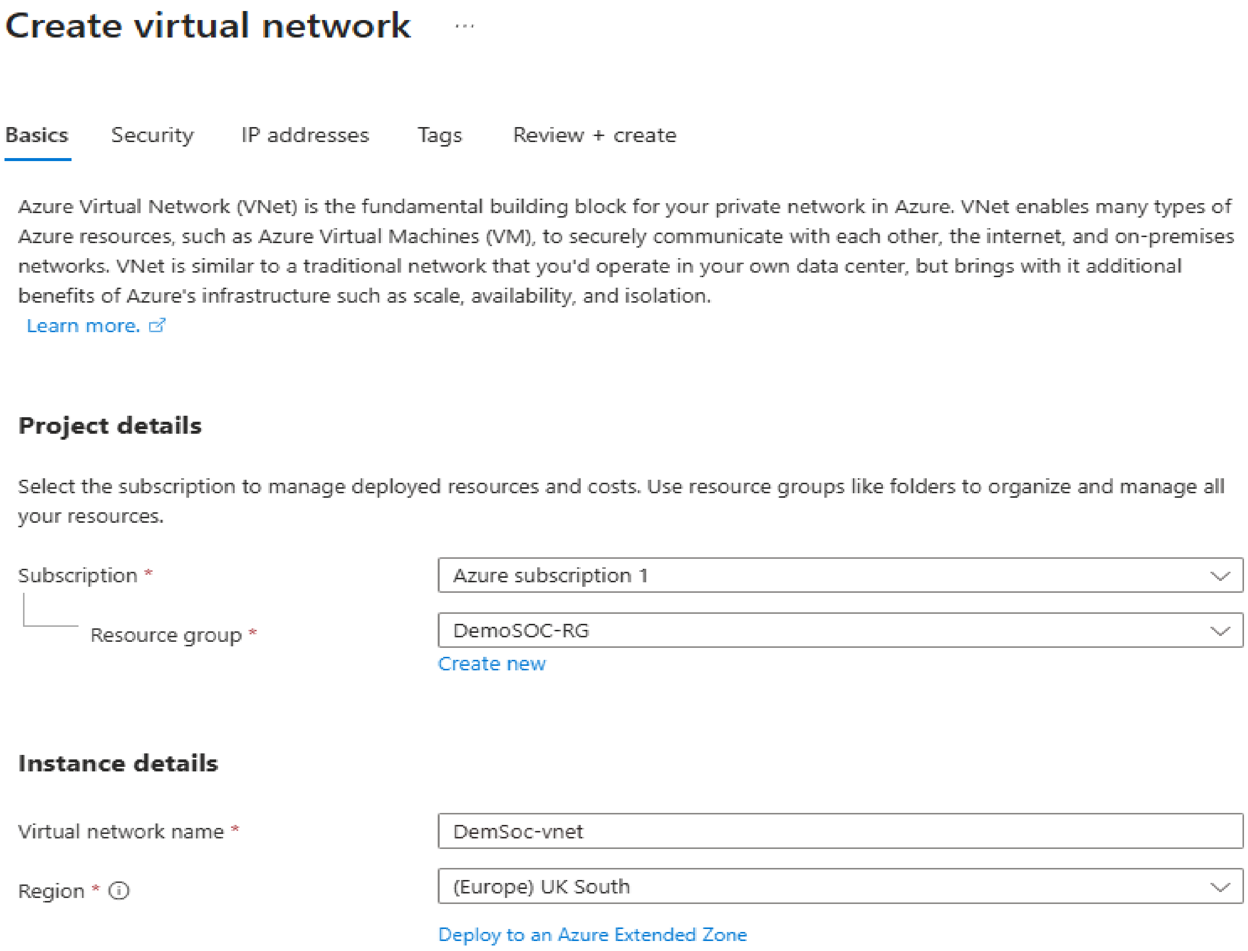
Subscription * ⓘ	Azure subscription 1
Resource group name * ⓘ	DemoSOC-RG
Region * ⓘ	(Europe) UK South

Fig 2

Create a Virtual Network (Vnet)

A Vnet is a logically isolated network inside Azure where you can securely run and connect Azure resources. Works the same way as an on-premises network but hosted in Azure.

Ensure the VNet is created under the resource group and region created in step 1



Create virtual network ···

Basics   Security   IP addresses   Tags   Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.
Learn more.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

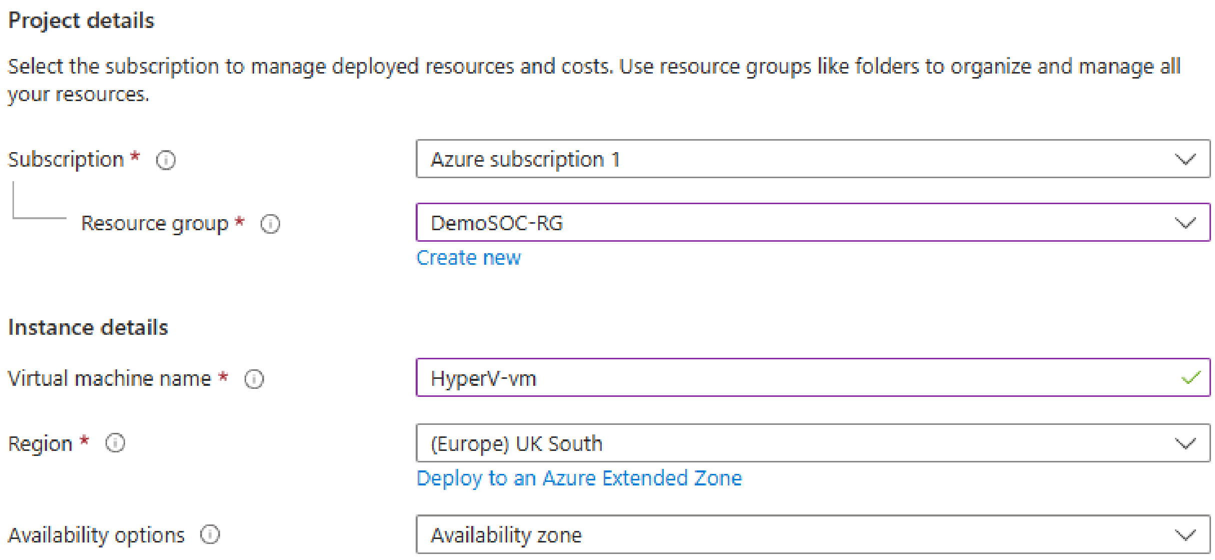
Subscription *	Azure subscription 1
Resource group *	DemoSOC-RG Create new

Instance details

Virtual network name *	DemSoc-vnet
Region * ⓘ	(Europe) UK South Deploy to an Azure Extended Zone

Fig 3

Create a Virtual Machine (VM)



Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Azure subscription 1

Resource group * : DemoSOC-RG

Instance details

Virtual machine name * : HyperV-vm ✓

Region * : (Europe) UK South

Availability options : Availability zone

Fig 4

Create the VM in the resource group and region in Step 1

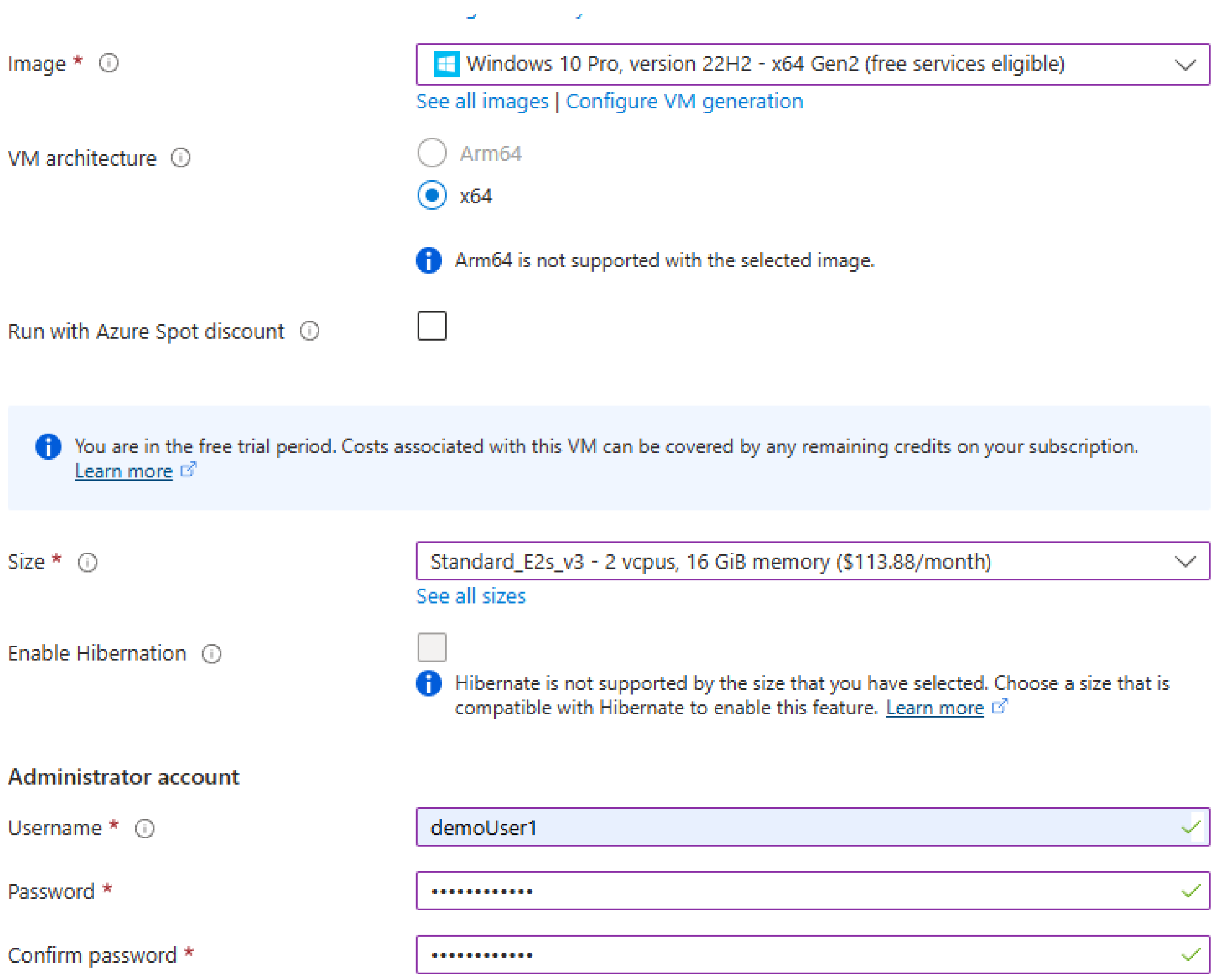


Image * ⓘ — Windows 10 Pro, version 22H2 - x64 Gen2 (free services eligible)

See all images | Configure VM generation

VM architecture ⓘ — ○ Arm64 ● x64

Arm64 is not supported with the selected image.

Run with Azure Spot discount ⓘ — □

You are in the free trial period. Costs associated with this VM can be covered by any remaining credits on your subscription. Learn more

Size * ⓘ — Standard_E2s_v3 - 2 vcpus, 16 GiB memory ($113.88/month)

See all sizes

Enable Hibernation ⓘ — □

Hibernate is not supported by the size that you have selected. Choose a size that is compatible with Hibernate to enable this feature. Learn more

Administrator account

Username * ⓘ — demoUser1 ✓

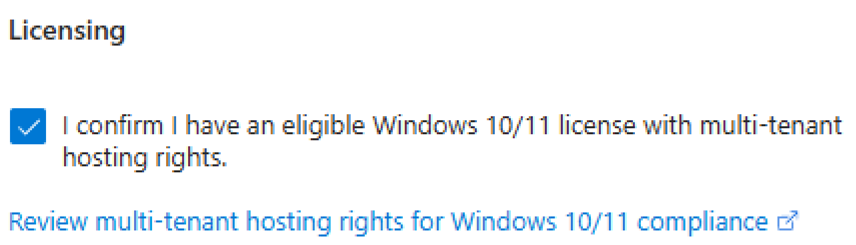
Password * — •••••••••••• ✓

Confirm password * — •••••••••••• ✓

Fig 5

In the Size use at least 2vcpus. Anything less will be painfully slow.

Ensure to confirm you have a license; otherwise, the process will not continue.



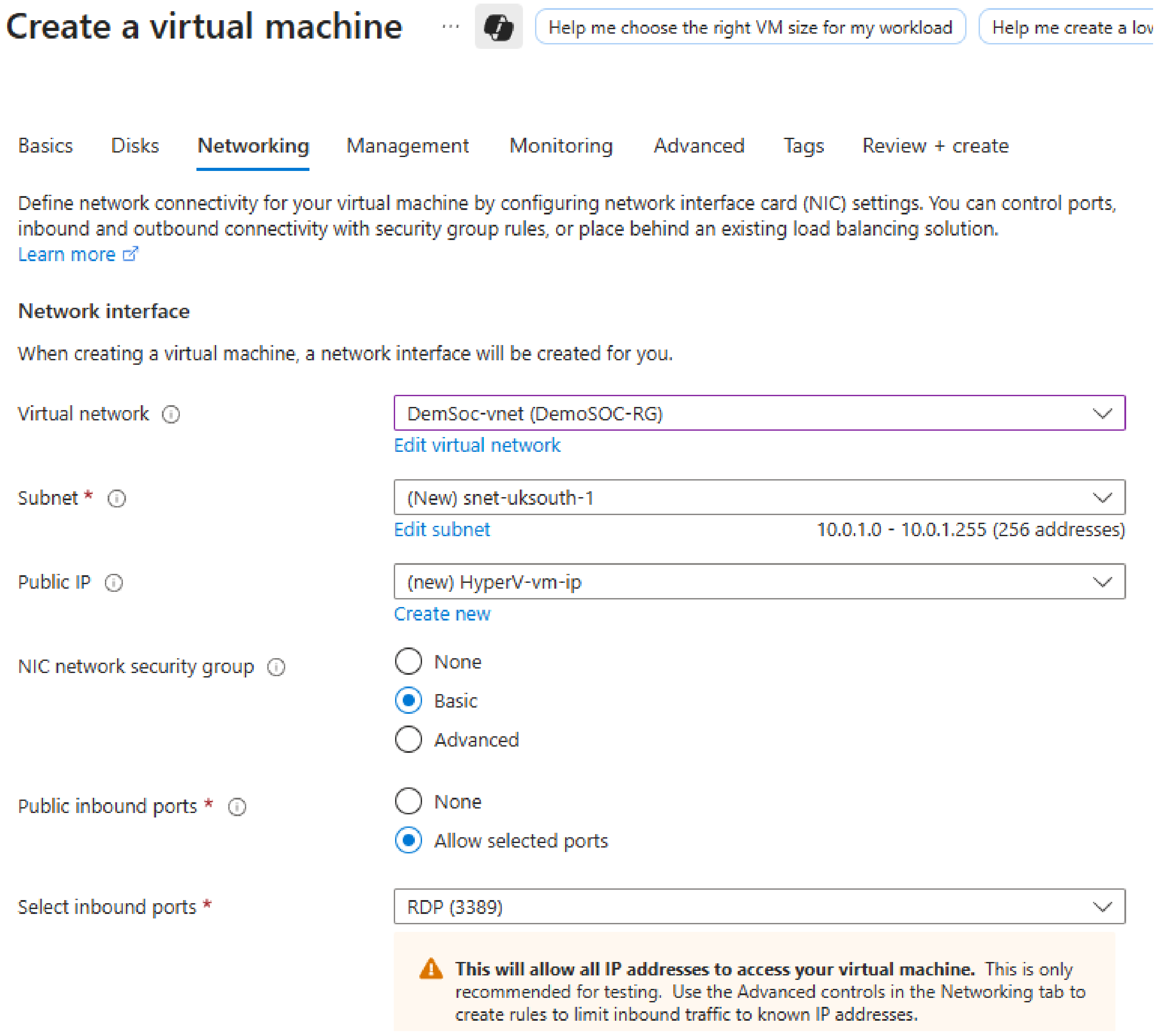
Licensing

☑ I confirm I have an eligible Windows 10/11 license with multi-tenant hosting rights.

Review multi-tenant hosting rights for Windows 10/11 compliance

Fig 6

In the Networking tab, select the Vnet created in the previous step.



Create a virtual machine ··· Help me choose the right VM size for my workload | Help me create a low

Basics | Disks | **Networking** | Management | Monitoring | Advanced | Tags | Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.
Learn more

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network: DemSoc-vnet (DemoSOC-RG)
Edit virtual network

Subnet *: (New) snet-uksouth-1
Edit subnet 10.0.1.0 - 10.0.1.255 (256 addresses)

Public IP: (new) HyperV-vm-ip
Create new

NIC network security group: ○ None ● Basic ○ Advanced

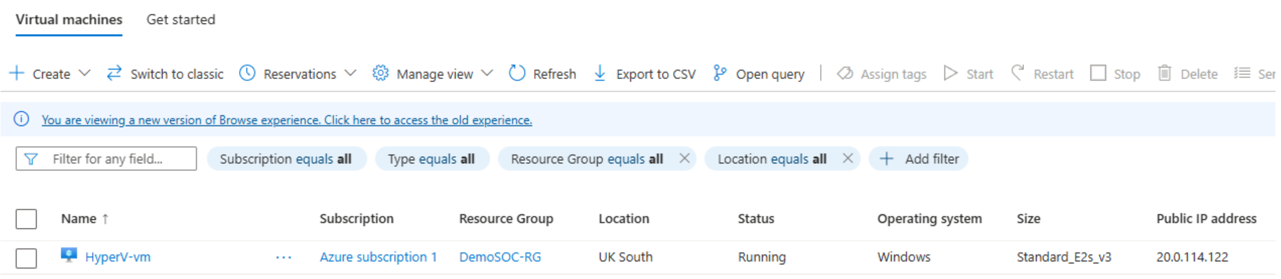
Public inbound ports *: ○ None ● Allow selected ports

Select inbound ports *: RDP (3389)

This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Fig 6

Click on Review and Create. Once the validation is passed, click create and wait for the VM to be provisioned.



Virtual machines | Get started

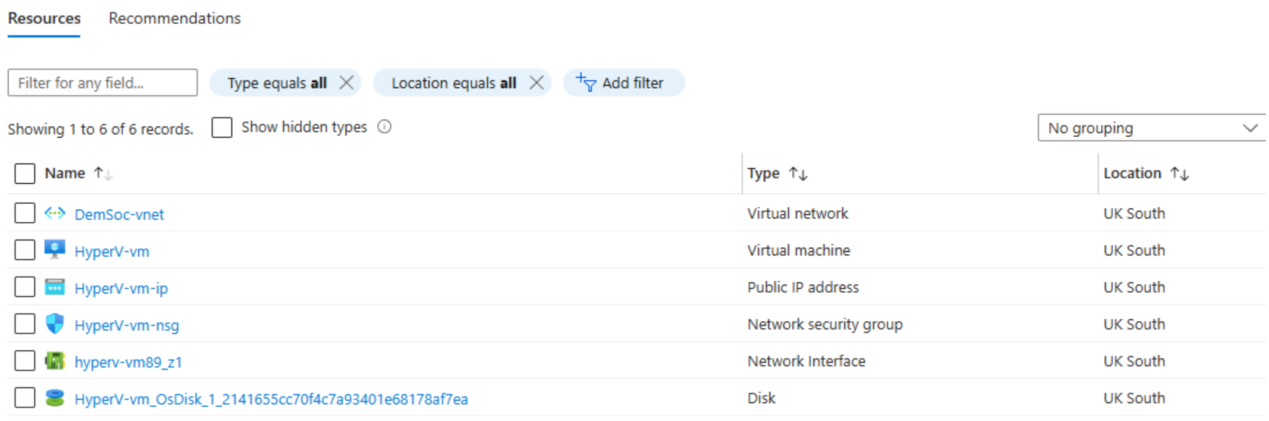
You are viewing a new version of Browse experience. Click here to access the old experience.

Filter for any field... | Subscription equals **all** | Type equals **all** | Resource Group equals **all** | Location equals **all** | + Add filter

☐	Name ↑	Subscription	Resource Group	Location	Status	Operating system	Size	Public IP address
☐	HyperV-vm	Azure subscription 1	DemoSOC-RG	UK South	Running	Windows	Standard_E2s_v3	20.0.114.122

Fig 7

With the VM created. Navigate to Home and click on Resource group. The following resources should be listed.



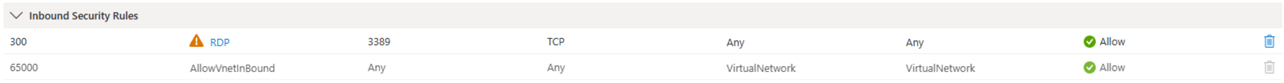
Showing 1 to 6 of 6 records. □ Show hidden types

□ Name ↑↓	Type ↑↓	Location ↑↓
□ DemSoc-vnet	Virtual network	UK South
□ HyperV-vm	Virtual machine	UK South
□ HyperV-vm-ip	Public IP address	UK South
□ HyperV-vm-nsg	Network security group	UK South
□ hyperv-vm89_z1	Network Interface	UK South
□ HyperV-vm_OsDisk_1_2141655cc70f4c7a93401e68178af7ea	Disk	UK South

Fig 8

Two resources were automatically created with the VM – HyperV-vm-nsg and HyperV-vm89_z1. Interest is in the NSG (Network Security Group), which acts like the firewall. We need to allow inbound traffic.

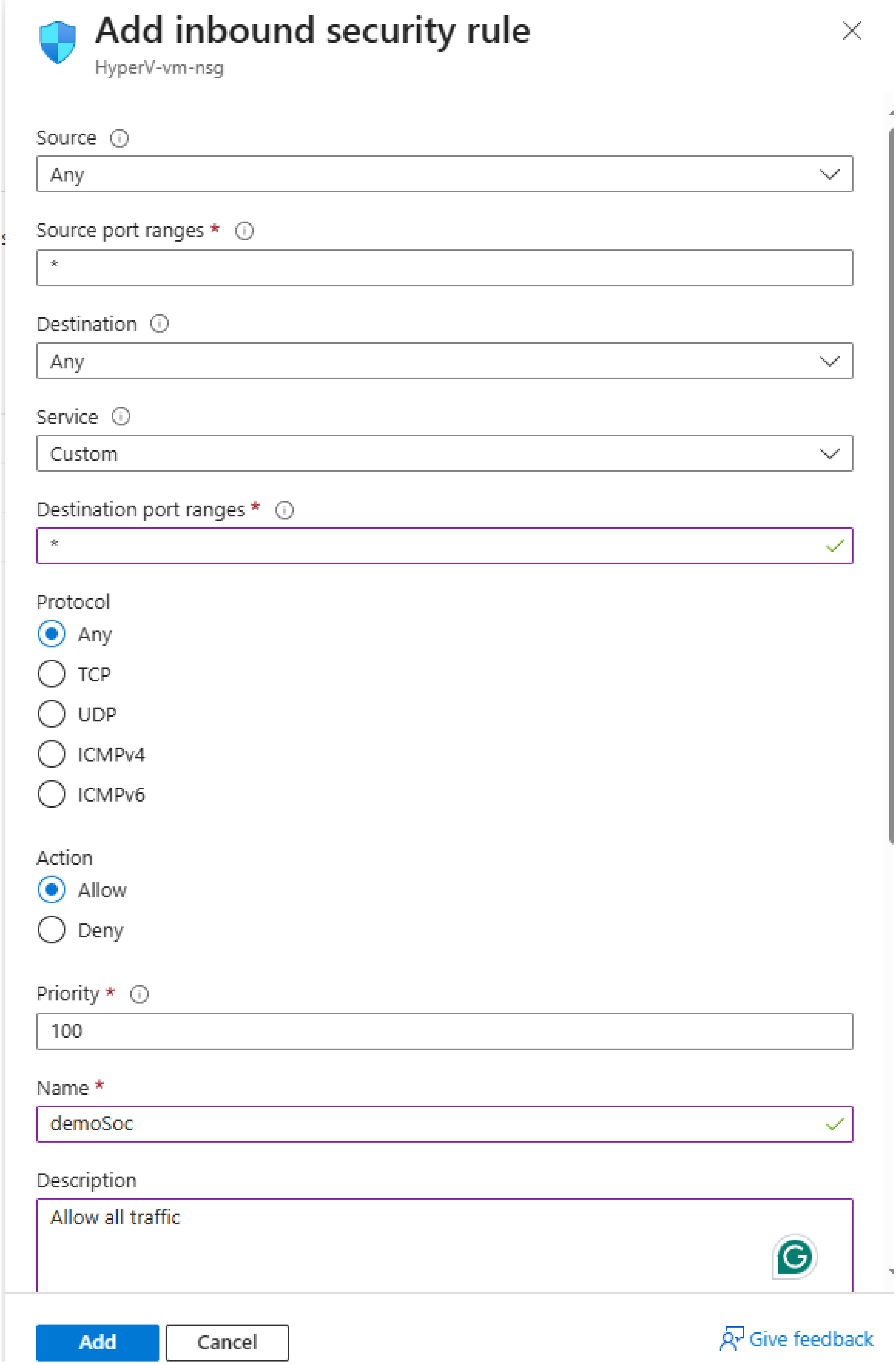
Delete the inbound rule with Priority Value 300 and create a new rule allowing any traffic from any destination.



Inbound Security Rules

300	⚠ RDP	3389	TCP	Any	Any	✓ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow

Fig 9



Add inbound security rule

HyperV-vm-nsg

Source: Any

Source port ranges *: *

Destination: Any

Service: Custom

Destination port ranges *: *

Protocol
- ● Any
- ○ TCP
- ○ UDP
- ○ ICMPv4
- ○ ICMPv6

Action
- ● Allow
- ○ Deny

Priority *: 100

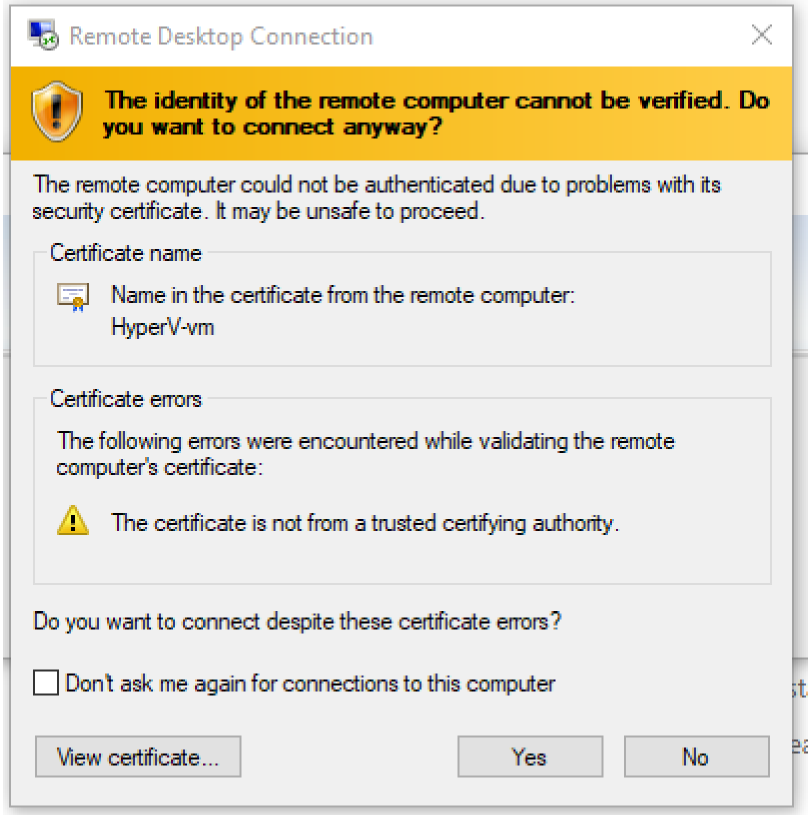
Name *: demoSoc

Description: Allow all traffic

Fig 10

Log into VM

With the inbound rule in place, log in to the computer via RDP. A successful login will present a certificate as shown below.



Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
HyperV-vm

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

□ Don't ask me again for connections to this computer

Fig 11

Click Yes on the Certificate, navigate to the Firewall settings, and deactivate the firewall. Right click on Windows Defender Firewall

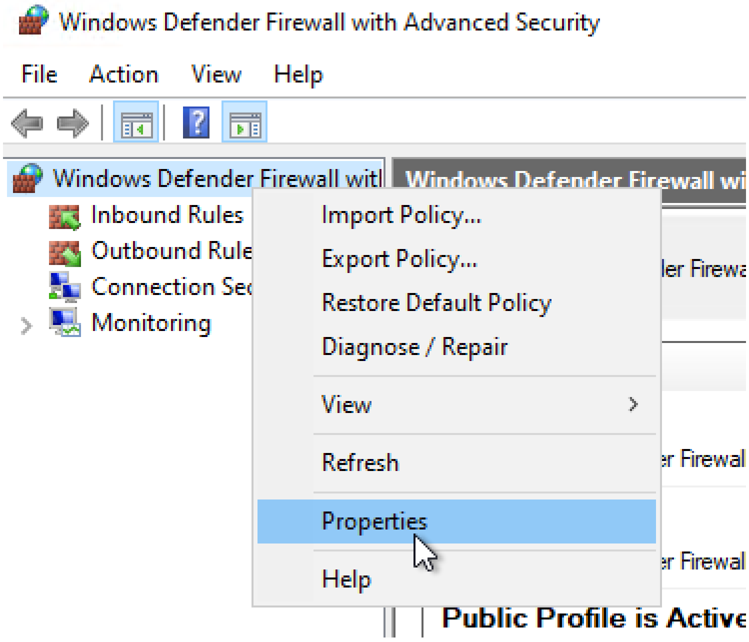
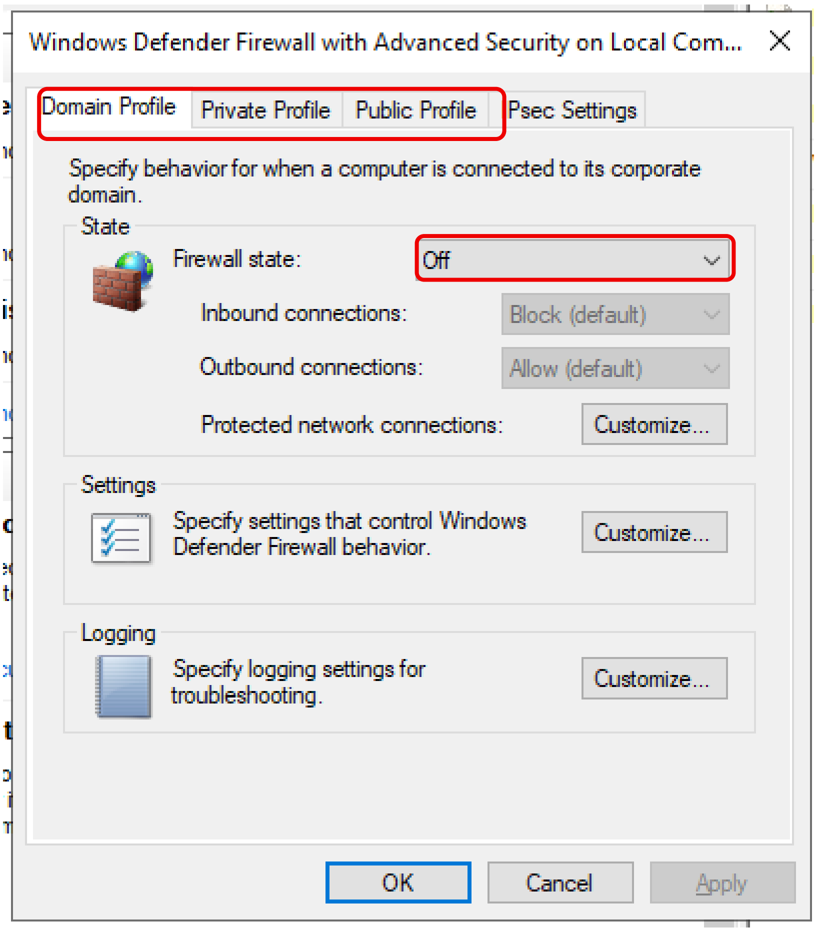


Fig 12

Disable the firewall state in all the tabs.



Windows Defender Firewall with Advanced Security on Local Com...

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: Off

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections: Customize...

Settings

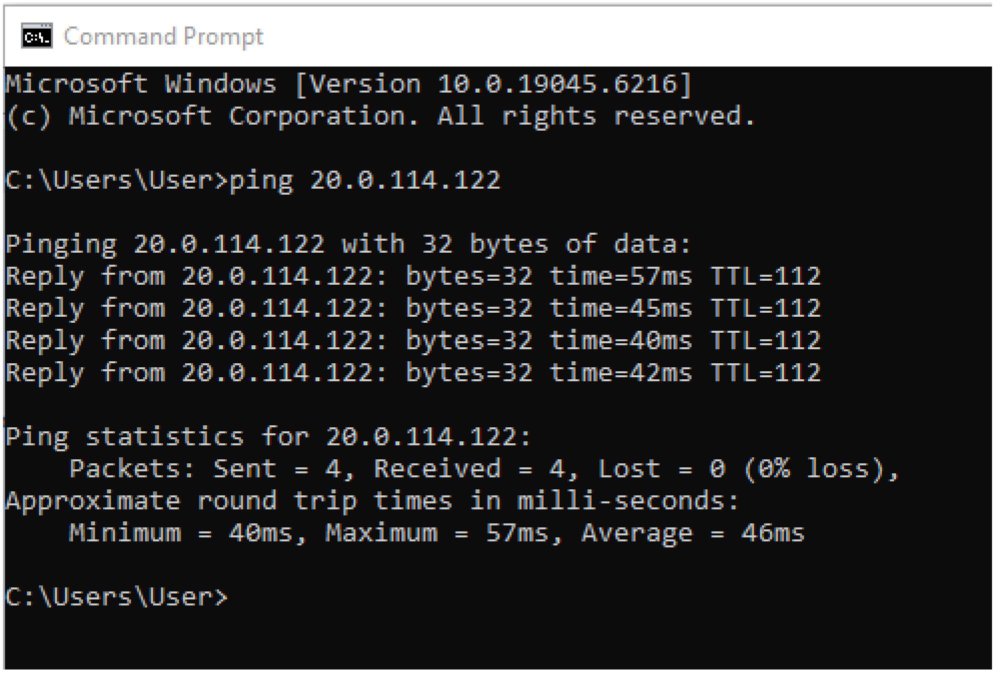
Specify settings that control Windows Defender Firewall behavior. Customize...

Logging

Specify logging settings for troubleshooting. Customize...

Fig 13

Test that you can reach the computer using a ping. This will show that if you can get a response, the public should be able to attack it.

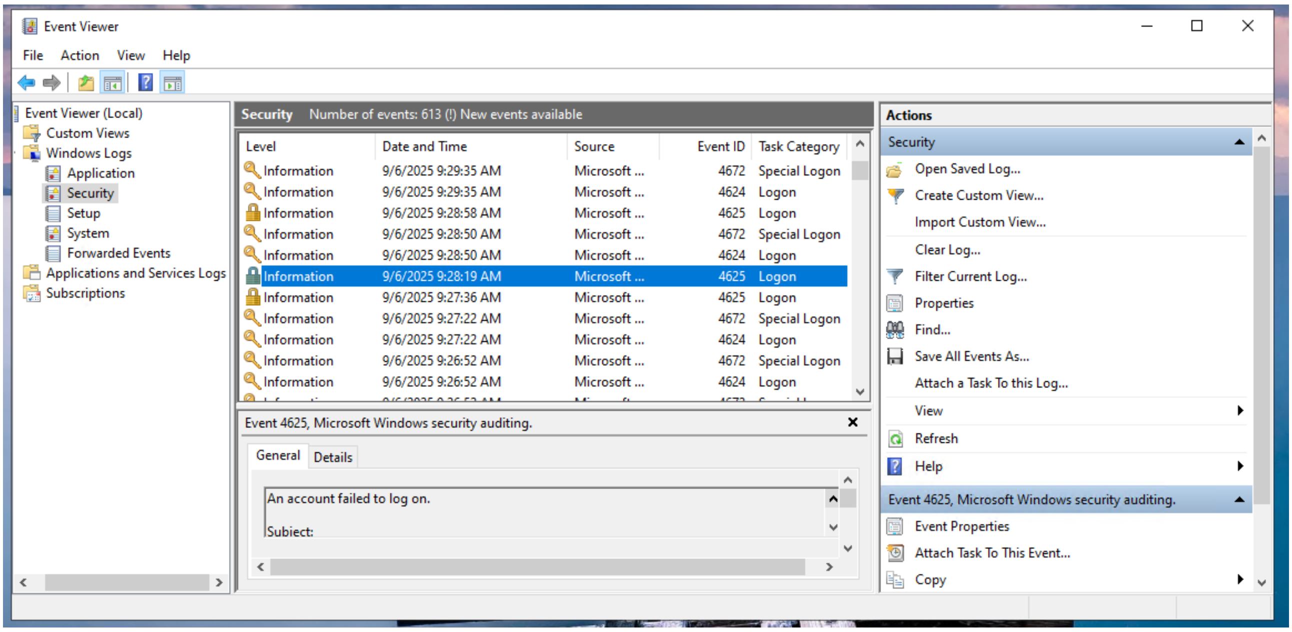


Command Prompt

```
Microsoft Windows [Version 10.0.19045.6216]
(c) Microsoft Corporation. All rights reserved.

C:\Users\User>ping 20.0.114.122

Pinging 20.0.114.122 with 32 bytes of data:
Reply from 20.0.114.122: bytes=32 time=57ms TTL=112
Reply from 20.0.114.122: bytes=32 time=45ms TTL=112
Reply from 20.0.114.122: bytes=32 time=40ms TTL=112
Reply from 20.0.114.122: bytes=32 time=42ms TTL=112

Ping statistics for 20.0.114.122:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 40ms, Maximum = 57ms, Average = 46ms

C:\Users\User>
```

Fig 14

Navigate to the Event viewer. This is where the activities on the computer are logged



Security Number of events: 613 (!) New events available

Level	Date and Time	Source	Event ID	Task Category
Information	9/6/2025 9:29:35 AM	Microsoft ...	4672	Special Logon
Information	9/6/2025 9:29:35 AM	Microsoft ...	4624	Logon
Information	9/6/2025 9:28:58 AM	Microsoft ...	4625	Logon
Information	9/6/2025 9:28:50 AM	Microsoft ...	4672	Special Logon
Information	9/6/2025 9:28:50 AM	Microsoft ...	4624	Logon
Information	9/6/2025 9:28:19 AM	Microsoft ...	4625	Logon
Information	9/6/2025 9:27:36 AM	Microsoft ...	4625	Logon
Information	9/6/2025 9:27:22 AM	Microsoft ...	4672	Special Logon
Information	9/6/2025 9:27:22 AM	Microsoft ...	4624	Logon
Information	9/6/2025 9:26:52 AM	Microsoft ...	4672	Special Logon
Information	9/6/2025 9:26:52 AM	Microsoft ...	4624	Logon

Event 4625, Microsoft Windows security auditing.

An account failed to log on.

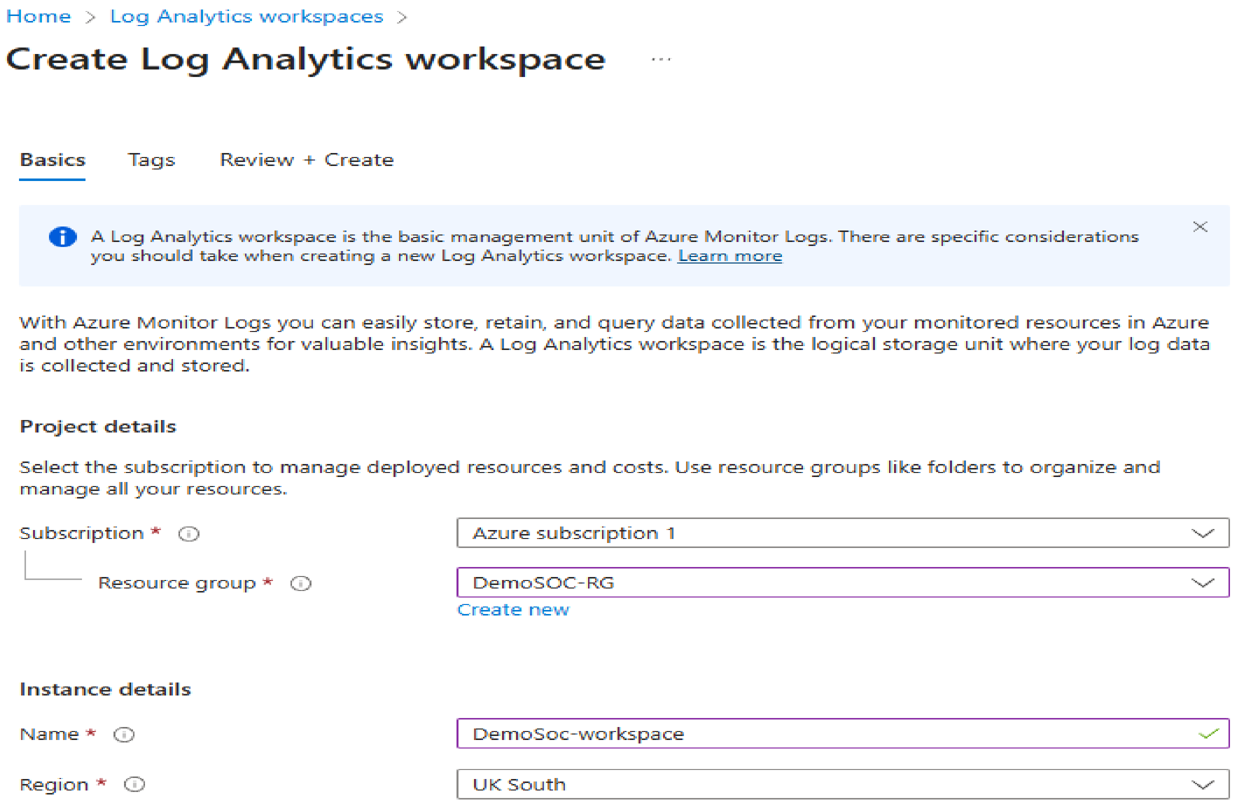
Subject:

Fig 15

Under Event ID, notice different events. These are the events that will be ingested into Sentinel.

Configure Sentinel

In Azure, in the search type Log Analytics to create a workspace. Which is a requirement for Sentinel



Home > Log Analytics workspaces >

Create Log Analytics workspace ...

A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. Learn more

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Azure subscription 1

Resource group * : DemoSOC-RG

Create new

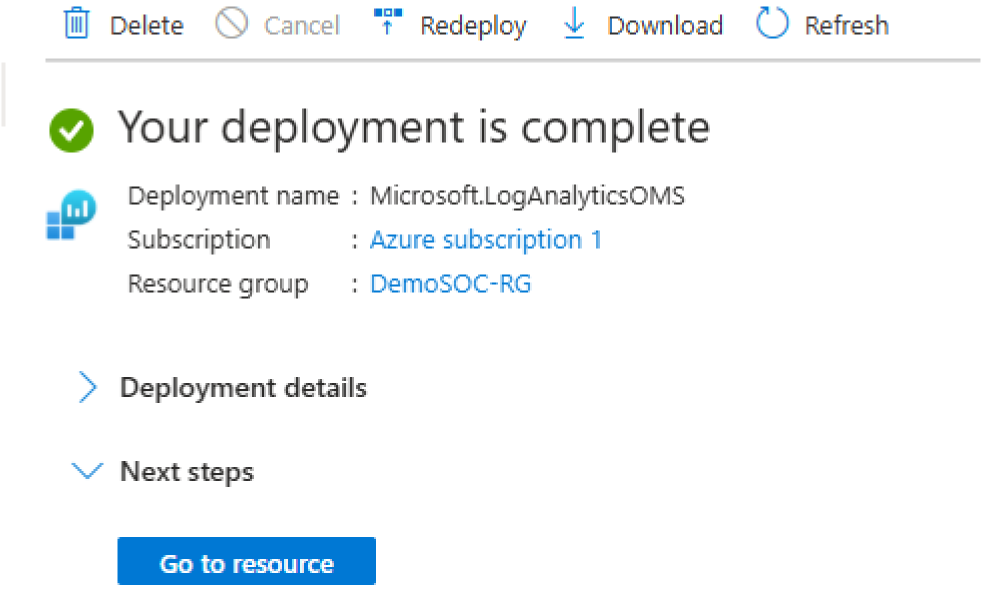
Instance details

Name * : DemoSoc-workspace

Region * : UK South

Fig 16

Create this in the same resource group and region as the VM



Your deployment is complete

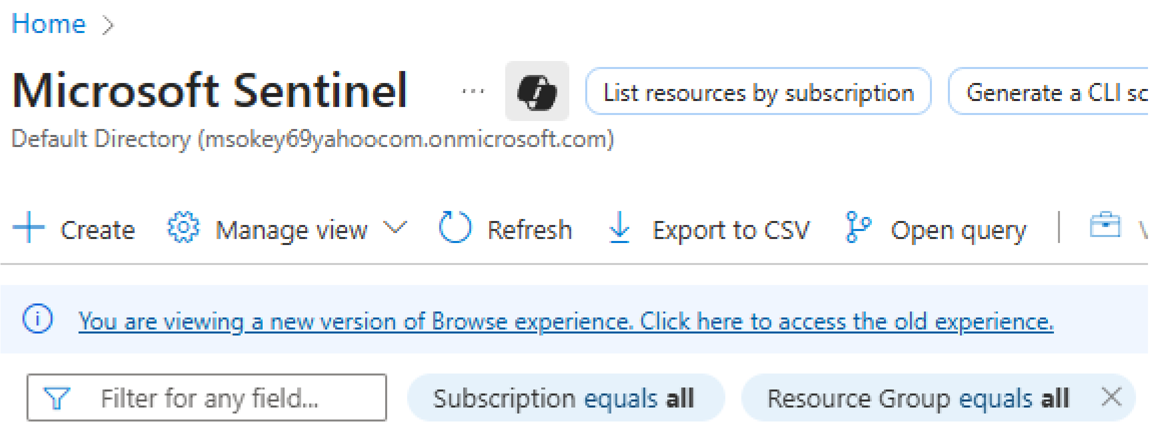
Deployment name : Microsoft.LogAnalyticsOMS

Subscription : Azure subscription 1

Resource group : DemoSOC-RG

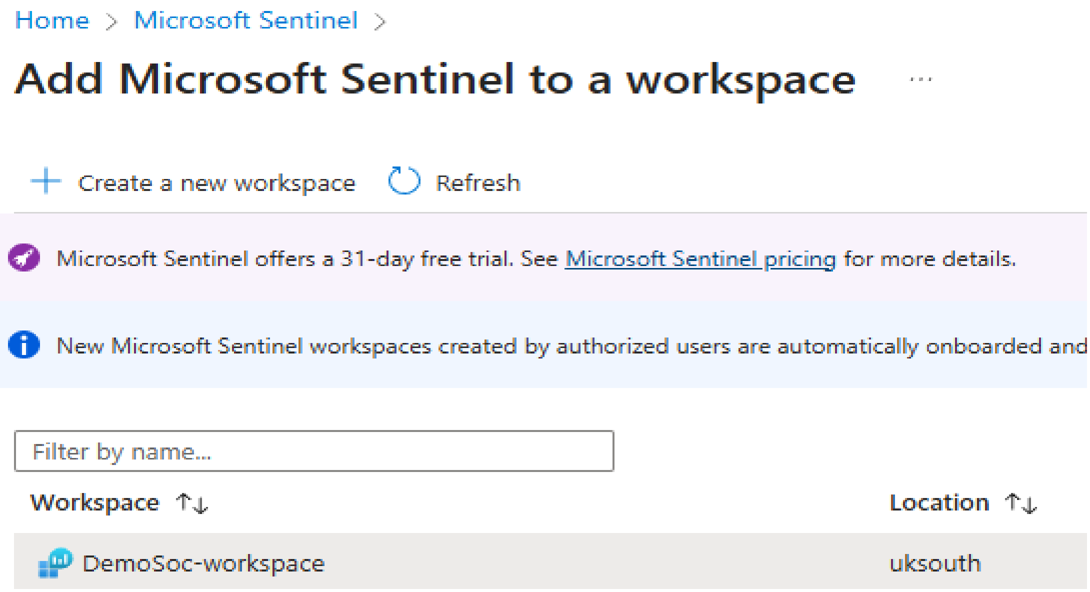
Fig 17

With the workspace created in the search space type Sentinel, click create



You are viewing a new version of Browse experience. Click here to access the old experience.

Fig 18


Home > Microsoft Sentinel >
Add Microsoft Sentinel to a workspace
Create a new workspace
Refresh
Filter by name...

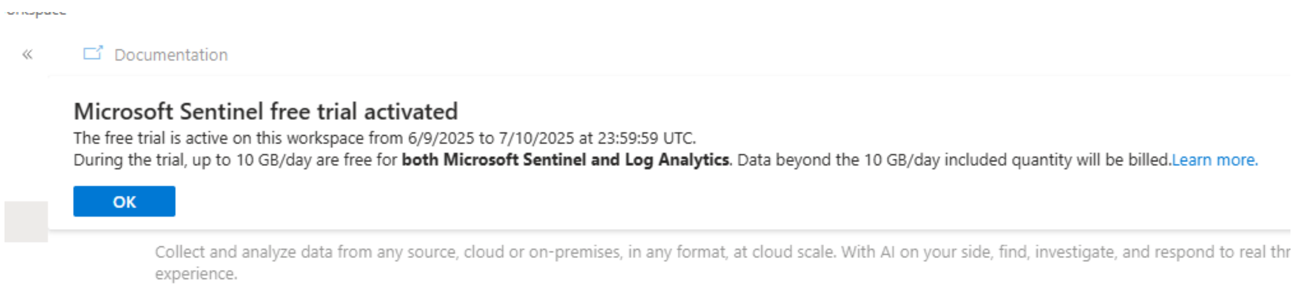
Microsoft Sentinel offers a 31-day free trial. See Microsoft Sentinel pricing for more details.

New Microsoft Sentinel workspaces created by authorized users are automatically onboarded and

Workspace ↑↓	Location ↑↓
DemoSoc-workspace	uksouth

Fig 19

Select the workspace created shown above



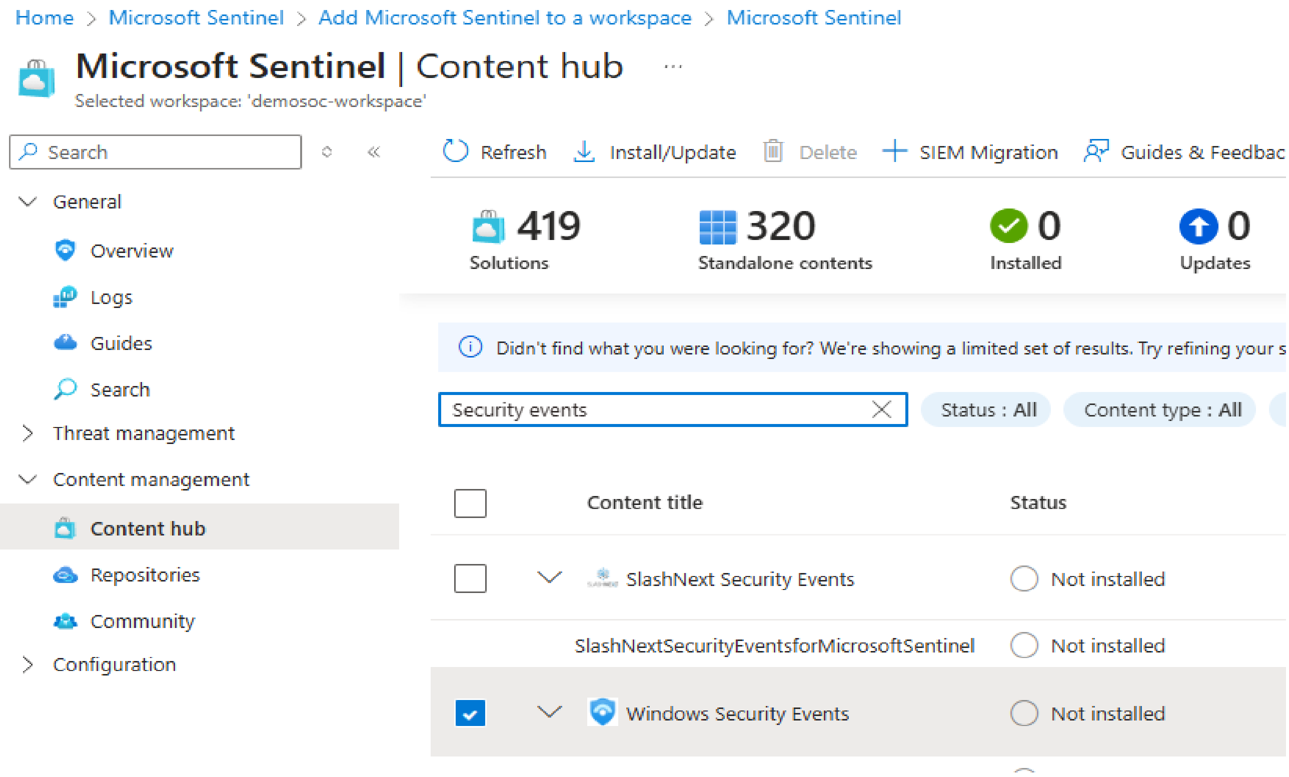
Microsoft Sentinel free trial activated

The free trial is active on this workspace from 6/9/2025 to 7/10/2025 at 23:59:59 UTC.
During the trial, up to 10 GB/day are free for **both Microsoft Sentinel and Log Analytics**. Data beyond the 10 GB/day included quantity will be billed.Learn more.

Collect and analyze data from any source, cloud or on-premises, in any format, at cloud scale. With AI on your side, find, investigate, and respond to real thr experience.

Fig 20

Navigate to the Content hub in Sentinel and search for security events



Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel

Microsoft Sentinel | Content hub ...

Selected workspace: 'demosoc-workspace'

Search

Refresh | Install/Update | Delete | SIEM Migration | Guides & Feedbac

419 Solutions | 320 Standalone contents | 0 Installed | 0 Updates

General
- Overview
- Logs
- Guides
- Search

Threat management

Content management
- Content hub
- Repositories
- Community

Configuration

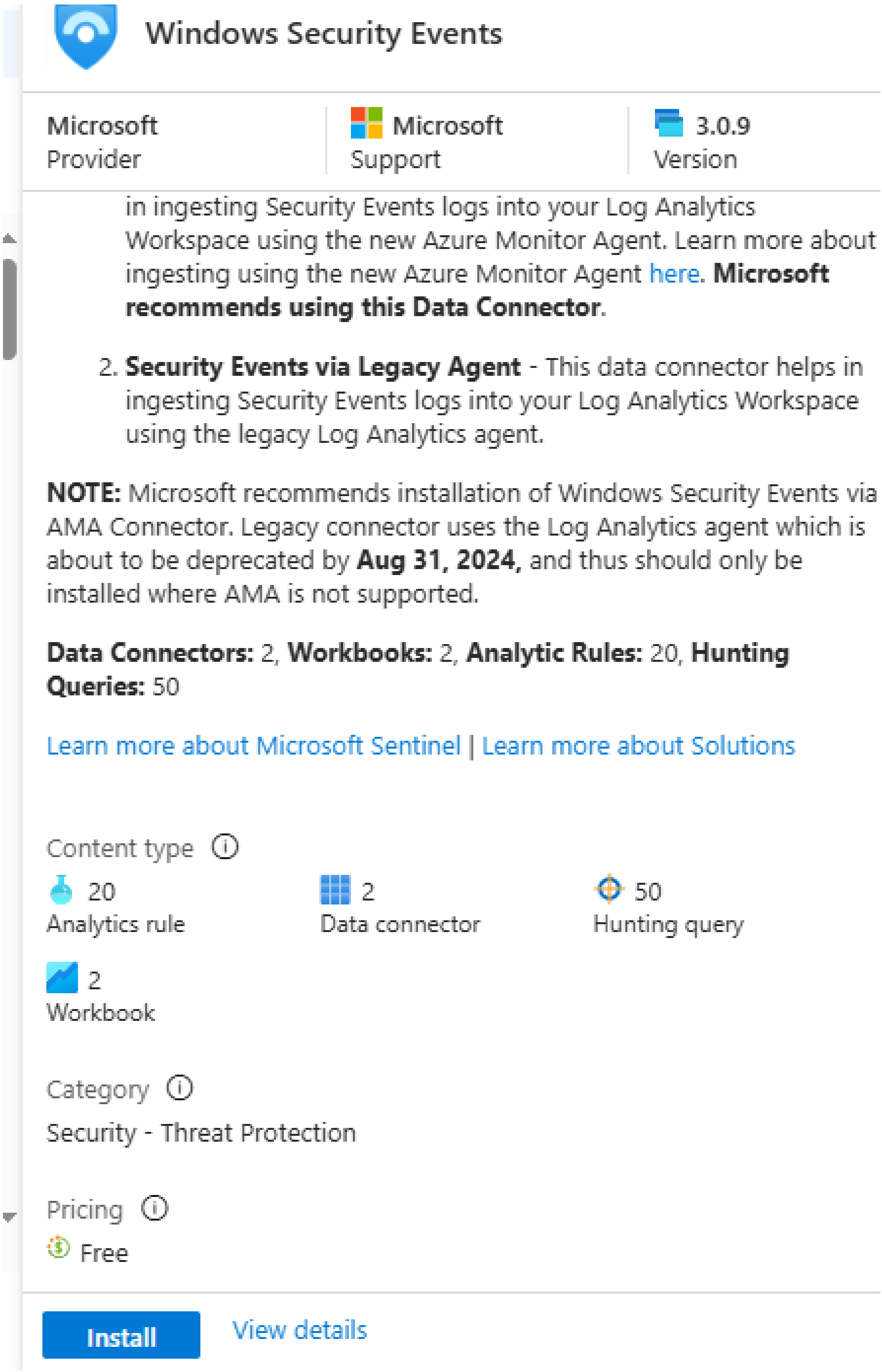
ⓘ Didn't find what you were looking for? We're showing a limited set of results. Try refining your s

Security events | Status : All | Content type : All

□		Content title	Status
□		SlashNext Security Events	○ Not installed
		SlashNextSecurityEventsforMicrosoftSentinel	○ Not installed
☑		Windows Security Events	○ Not installed

Fig 21

Select Windows Security Events. At the bottom of the page, on the right-hand click on the install button.



Windows Security Events

Microsoft
Provider

Microsoft
Support

3.0.9
Version

in ingesting Security Events logs into your Log Analytics Workspace using the new Azure Monitor Agent. Learn more about ingesting using the new Azure Monitor Agent here. **Microsoft recommends using this Data Connector**.

2. **Security Events via Legacy Agent** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the legacy Log Analytics agent.

NOTE: Microsoft recommends installation of Windows Security Events via AMA Connector. Legacy connector uses the Log Analytics agent which is about to be deprecated by **Aug 31, 2024,** and thus should only be installed where AMA is not supported.

Data Connectors: 2, **Workbooks:** 2, **Analytic Rules:** 20, **Hunting Queries:** 50

Learn more about Microsoft Sentinel | Learn more about Solutions

Content type

20
Analytics rule

2
Data connector

50
Hunting query

2
Workbook

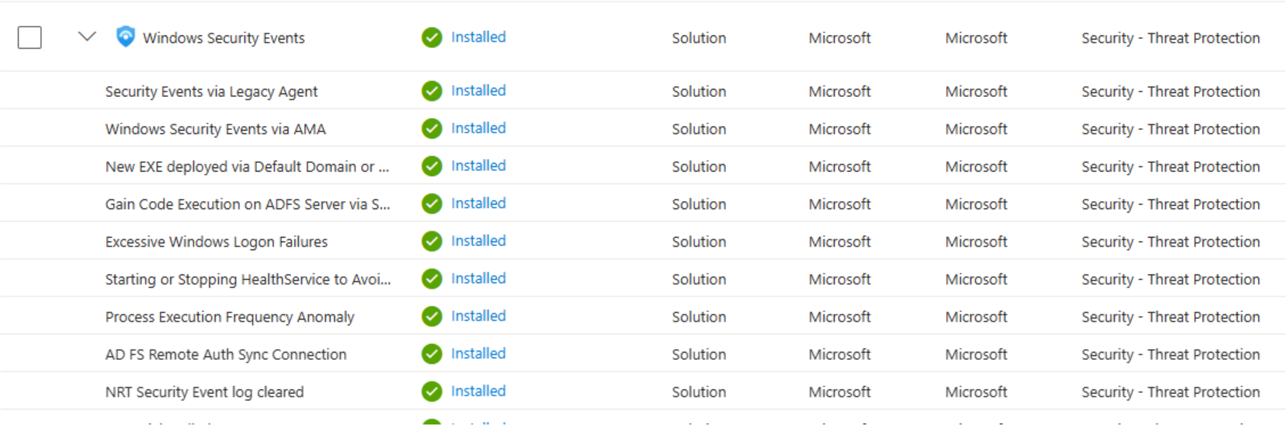
Category

Security - Threat Protection

Pricing

Free

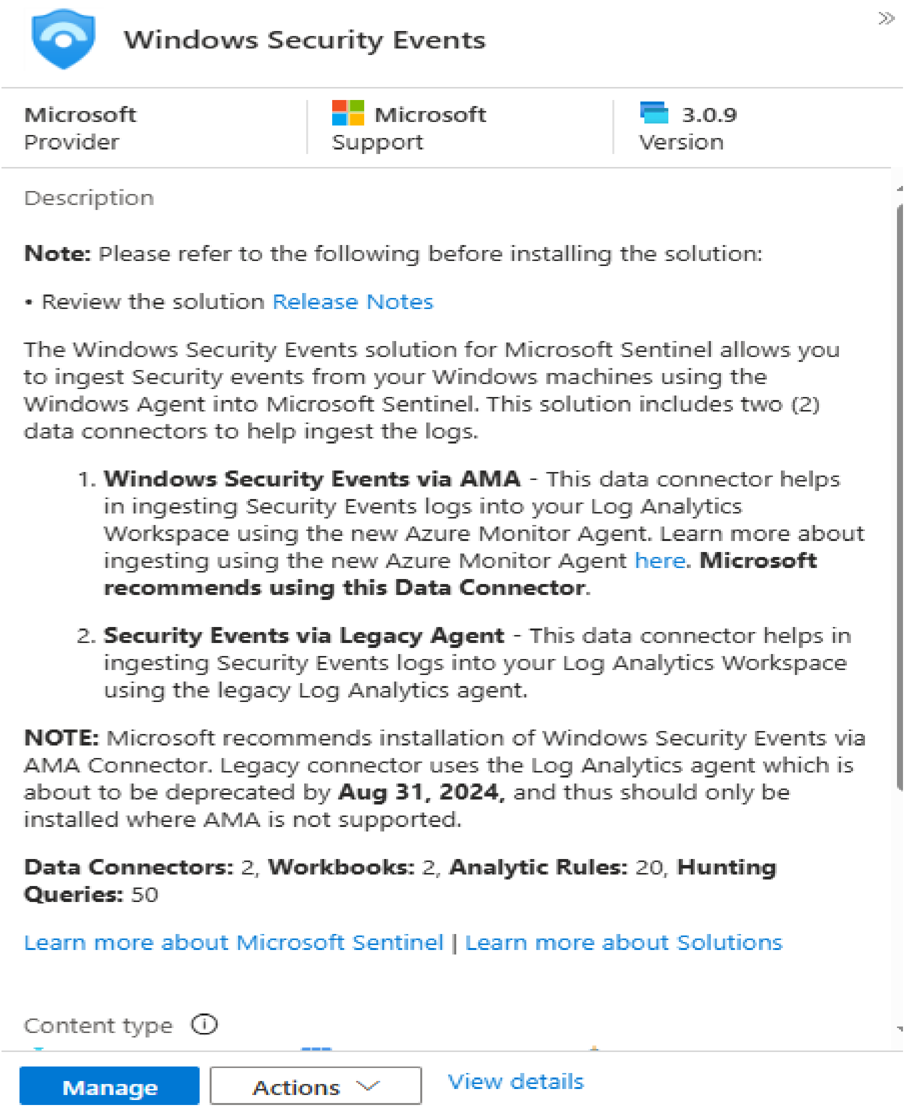
Fig 22



□ Windows Security Events	✓ Installed	Solution	Microsoft	Microsoft	Security - Threat Protection
Security Events via Legacy Agent	✓ Installed	Solution	Microsoft	Microsoft	Security - Threat Protection
Windows Security Events via AMA	✓ Installed	Solution	Microsoft	Microsoft	Security - Threat Protection
New EXE deployed via Default Domain or ...	✓ Installed	Solution	Microsoft	Microsoft	Security - Threat Protection
Gain Code Execution on ADFS Server via S...	✓ Installed	Solution	Microsoft	Microsoft	Security - Threat Protection
Excessive Windows Logon Failures	✓ Installed	Solution	Microsoft	Microsoft	Security - Threat Protection
Starting or Stopping HealthService to Avoi...	✓ Installed	Solution	Microsoft	Microsoft	Security - Threat Protection
Process Execution Frequency Anomaly	✓ Installed	Solution	Microsoft	Microsoft	Security - Threat Protection
AD FS Remote Auth Sync Connection	✓ Installed	Solution	Microsoft	Microsoft	Security - Threat Protection
NRT Security Event log cleared	✓ Installed	Solution	Microsoft	Microsoft	Security - Threat Protection

Fig 23

Click on Manage



Windows Security Events

Microsoft
Provider

Microsoft
Support

3.0.9
Version

Description

Note: Please refer to the following before installing the solution:

- Review the solution Release Notes

The Windows Security Events solution for Microsoft Sentinel allows you to ingest Security events from your Windows machines using the Windows Agent into Microsoft Sentinel. This solution includes two (2) data connectors to help ingest the logs.

1. **Windows Security Events via AMA** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the new Azure Monitor Agent. Learn more about ingesting using the new Azure Monitor Agent here. **Microsoft recommends using this Data Connector**.
2. **Security Events via Legacy Agent** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the legacy Log Analytics agent.

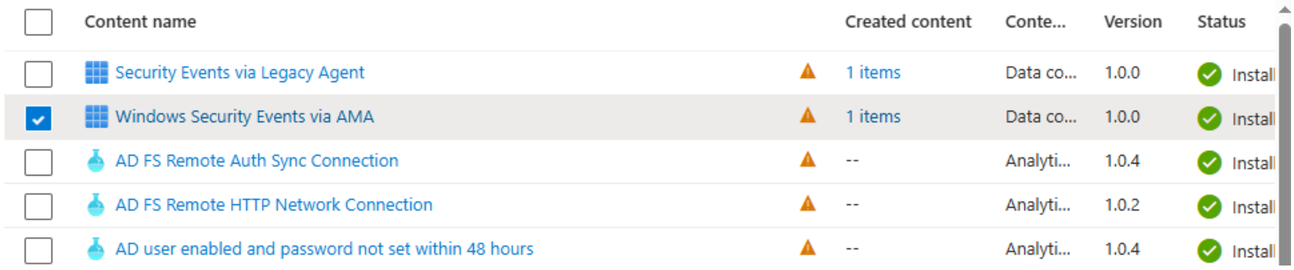
NOTE: Microsoft recommends installation of Windows Security Events via AMA Connector. Legacy connector uses the Log Analytics agent which is about to be deprecated by **Aug 31, 2024,** and thus should only be installed where AMA is not supported.

Data Connectors: 2, **Workbooks:** 2, **Analytic Rules:** 20, **Hunting Queries:** 50

Learn more about Microsoft Sentinel | Learn more about Solutions

Content type ⓘ

Fig 24

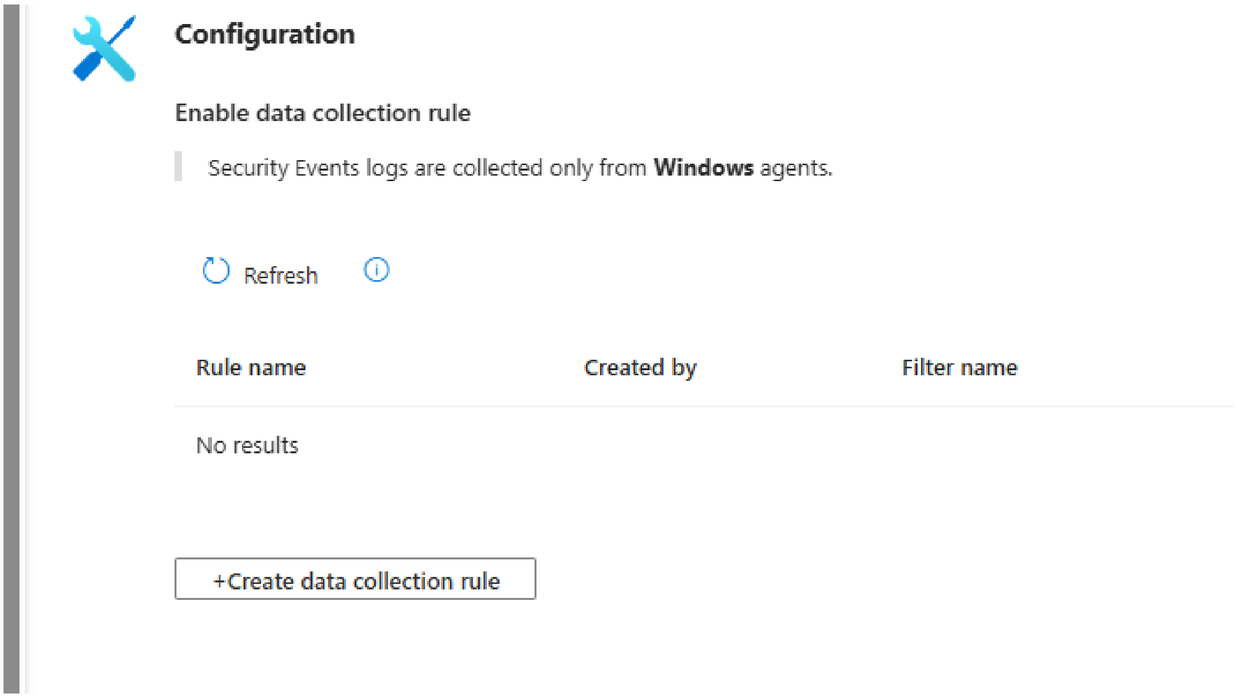


☐	Content name		Created content	Conte...	Version	Status
☐	Security Events via Legacy Agent	⚠	1 items	Data co...	1.0.0	✓ Install
☑	Windows Security Events via AMA	⚠	1 items	Data co...	1.0.0	✓ Install
☐	AD FS Remote Auth Sync Connection	⚠	--	Analyti...	1.0.4	✓ Install
☐	AD FS Remote HTTP Network Connection	⚠	--	Analyti...	1.0.2	✓ Install
☐	AD user enabled and password not set within 48 hours	⚠	--	Analyti...	1.0.4	✓ Install

Fig 25

Configure the collection rule.

Click on Create data collection rule. This rule instructs the VM to forward the Event logs to the log analytics workspace



Configuration

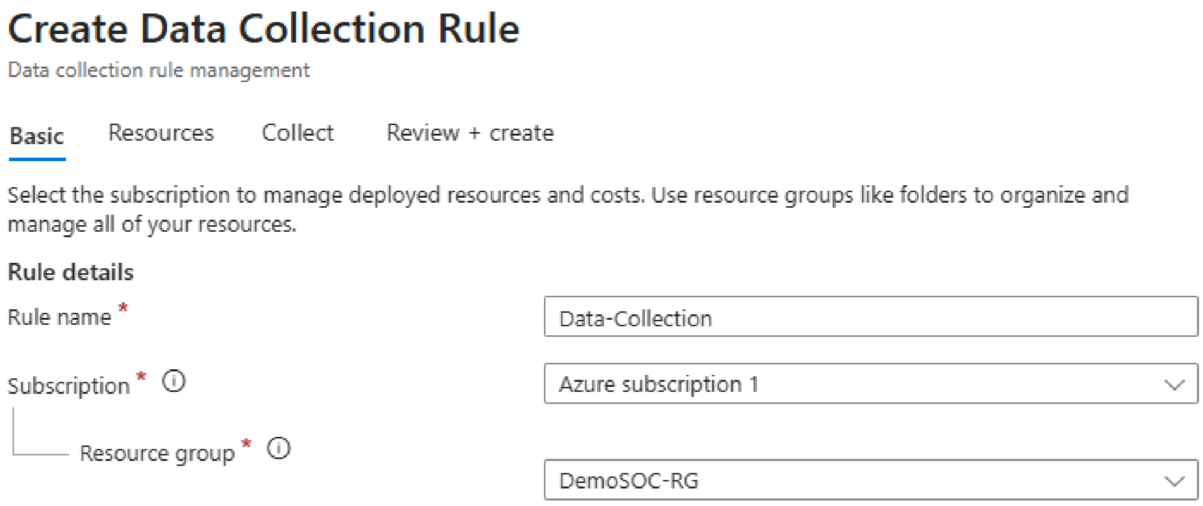
Enable data collection rule

Security Events logs are collected only from **Windows** agents.

Rule name	Created by	Filter name
No results		

Fig 26

Give the collection rule a name. select the resource group



Create Data Collection Rule

Data collection rule management

Basic | Resources | Collect | Review + create

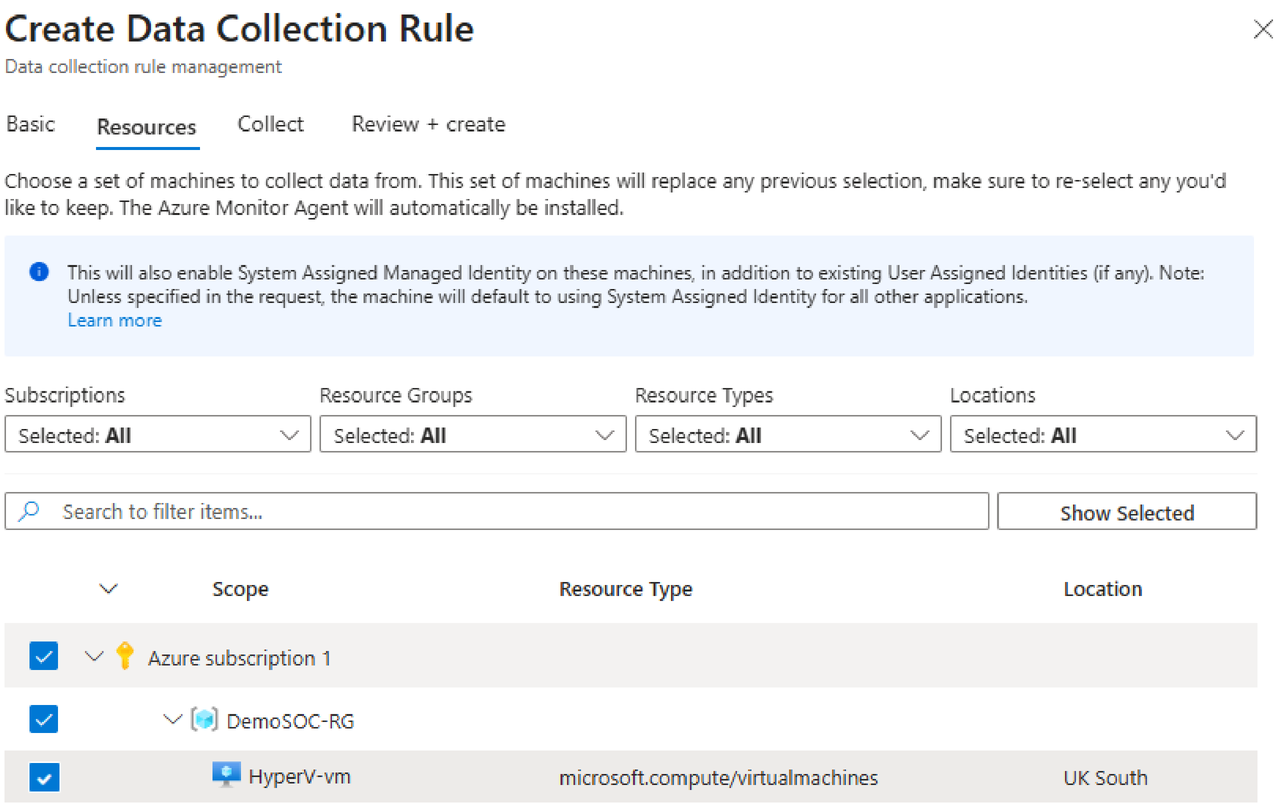
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all of your resources.

Rule details

Rule name *	Data-Collection
Subscription * ⓘ	Azure subscription 1
Resource group * ⓘ	DemoSOC-RG

Fig 27

Select the device whose event log will be ingested



Create Data Collection Rule

Data collection rule management

Basic | Resources | Collect | Review + create

Choose a set of machines to collect data from. This set of machines will replace any previous selection, make sure to re-select any you'd like to keep. The Azure Monitor Agent will automatically be installed.

This will also enable System Assigned Managed Identity on these machines, in addition to existing User Assigned Identities (if any). Note: Unless specified in the request, the machine will default to using System Assigned Identity for all other applications.
Learn more

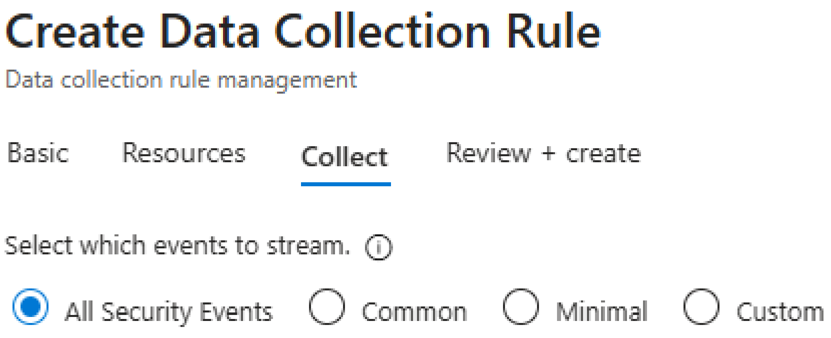
Subscriptions	Resource Groups	Resource Types	Locations
Selected: **All**	Selected: **All**	Selected: **All**	Selected: **All**

Search to filter items... | Show Selected

	Scope	Resource Type	Location
☑	Azure subscription 1		
☑	DemoSOC-RG		
☑	HyperV-vm	microsoft.compute/virtualmachines	UK South

Fig 28

Ensure All security radio is checked.



Create Data Collection Rule

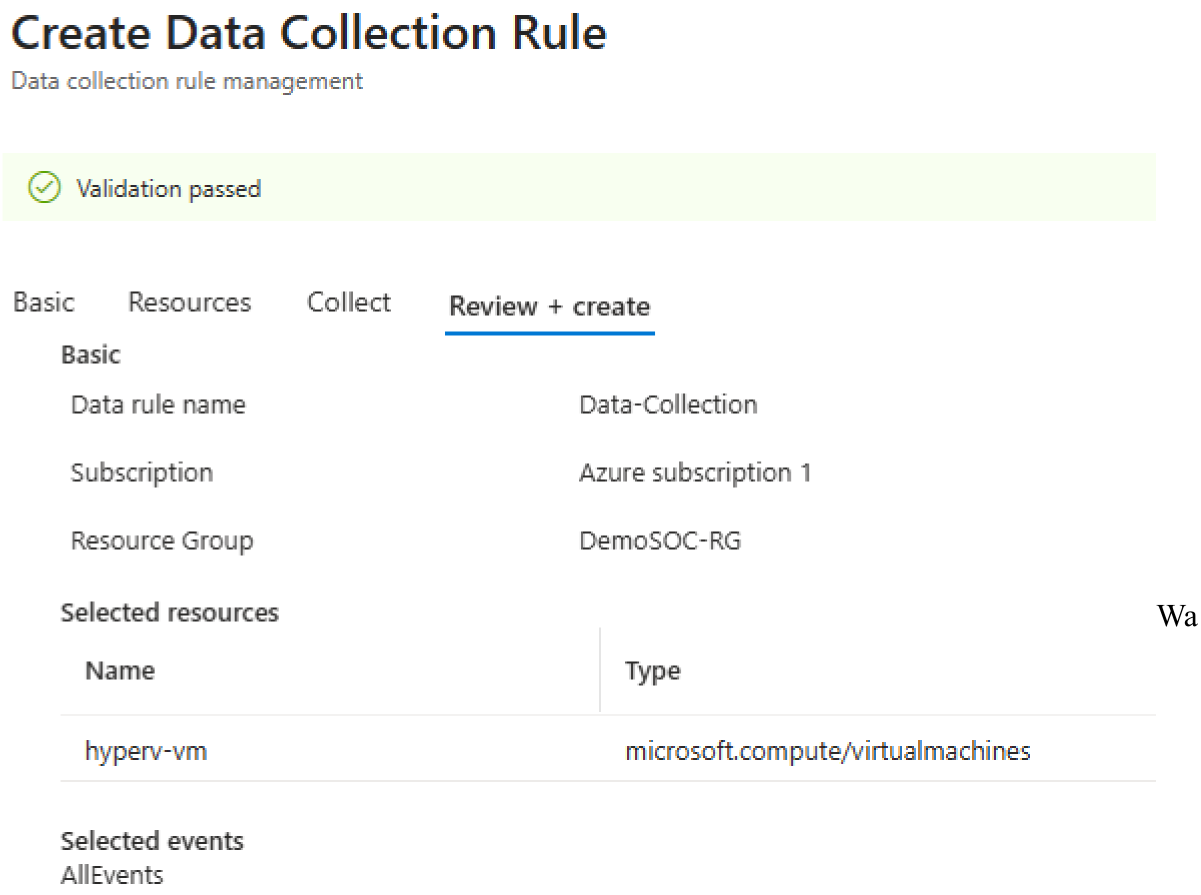
Data collection rule management

Select which events to stream.

● All Security Events ○ Common ○ Minimal ○ Custom

Fig 29

Review and create the rule.



Create Data Collection Rule

Data collection rule management

Validation passed

Basic

Data rule name	Data-Collection
Subscription	Azure subscription 1
Resource Group	DemoSOC-RG

Selected resources

Name	Type
hyperv-vm	microsoft.compute/virtualmachines

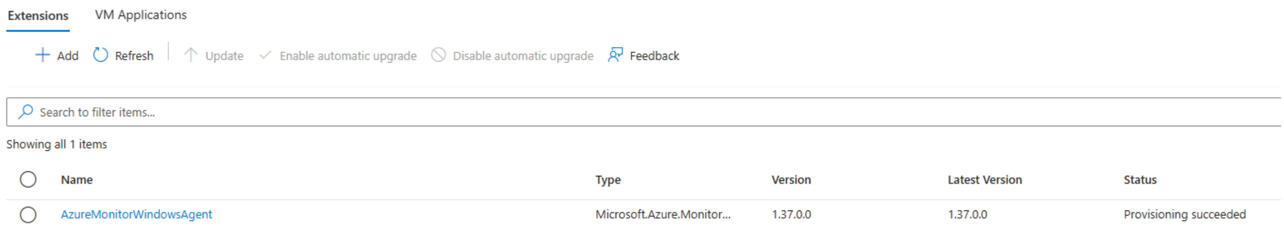
Selected events

AllEvents

Wa

Fig 30

Give the provisioning of the agent time to complete.



Showing all 1 items

Name	Type	Version	Latest Version	Status
AzureMonitorWindowsAgent	Microsoft.Azure.Monitor...	1.37.0.0	1.37.0.0	Provisioning succeeded

Fig 31

On the Log Analytics workspace page, click on Logs. In the right-hand corner of the drop-down menu, select KQL query

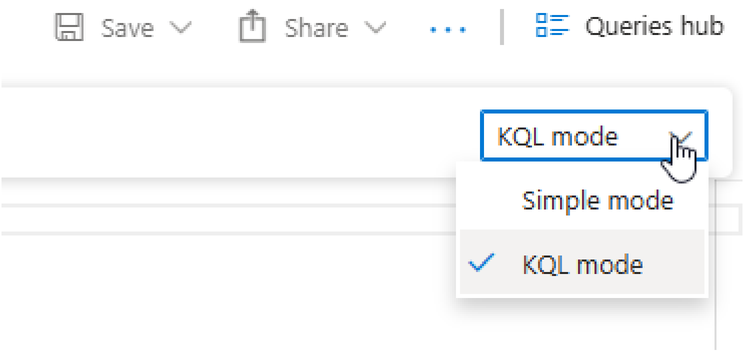
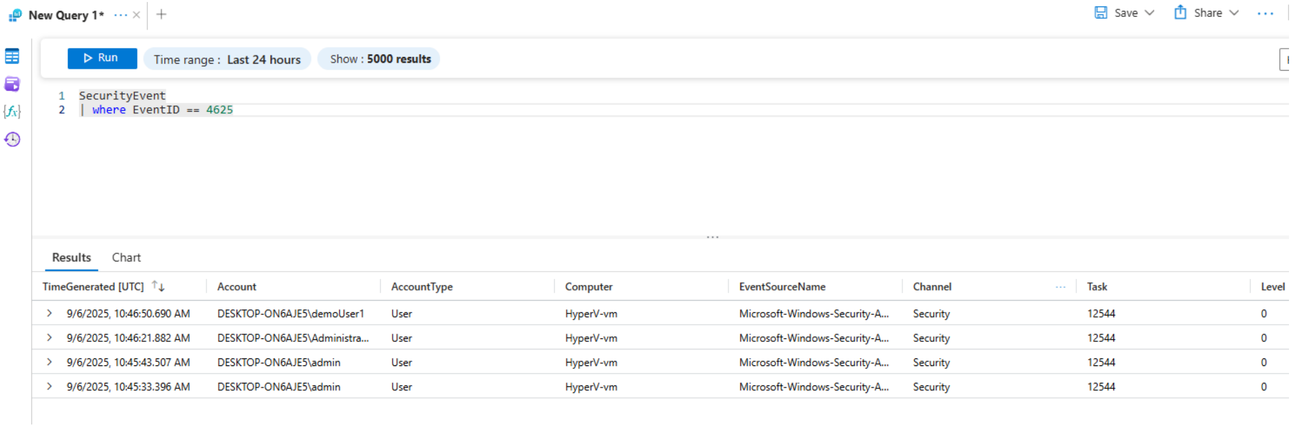


Fig 32

Write a query to display failed logins on the VM:
SecurityEvent
| where EventID == 4625



Time range : Last 24 hours

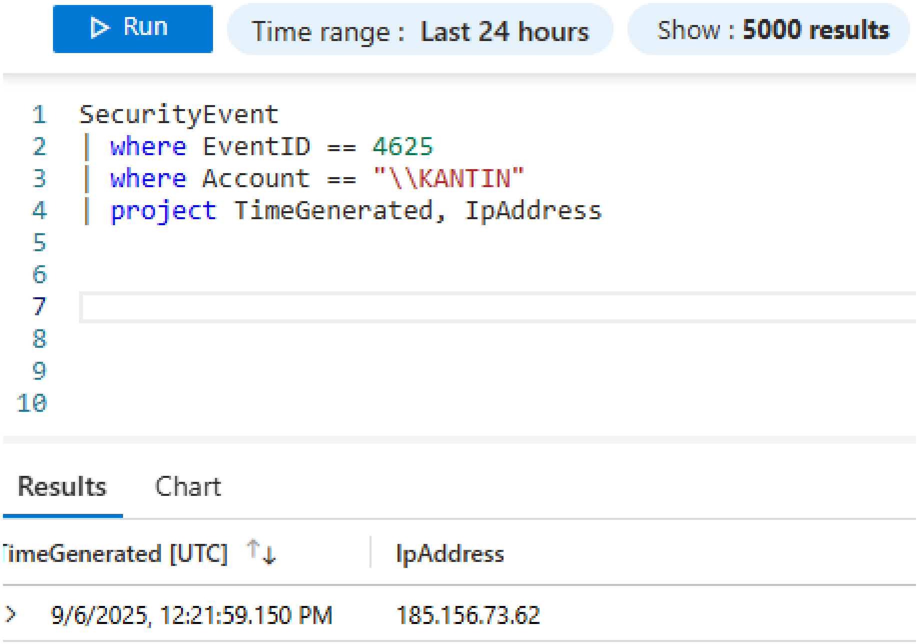
Show : 5000 results

```
SecurityEvent
| where EventID == 4625
```

TimeGenerated [UTC]	Account	AccountType	Computer	EventSourceName	Channel	Task	Level
9/6/2025, 10:46:50.690 AM	DESKTOP-ON6AJE5\demoUser1	User	HyperV-vm	Microsoft-Windows-Security-A...	Security	12544	0
9/6/2025, 10:46:21.882 AM	DESKTOP-ON6AJE5\Administra...	User	HyperV-vm	Microsoft-Windows-Security-A...	Security	12544	0
9/6/2025, 10:45:43.507 AM	DESKTOP-ON6AJE5\admin	User	HyperV-vm	Microsoft-Windows-Security-A...	Security	12544	0
9/6/2025, 10:45:33.396 AM	DESKTOP-ON6AJE5\admin	User	HyperV-vm	Microsoft-Windows-Security-A...	Security	12544	0

Fig 33

Run a few more queries to make sure the data is being ingested.



Time range : Last 24 hours

Show : 5000 results

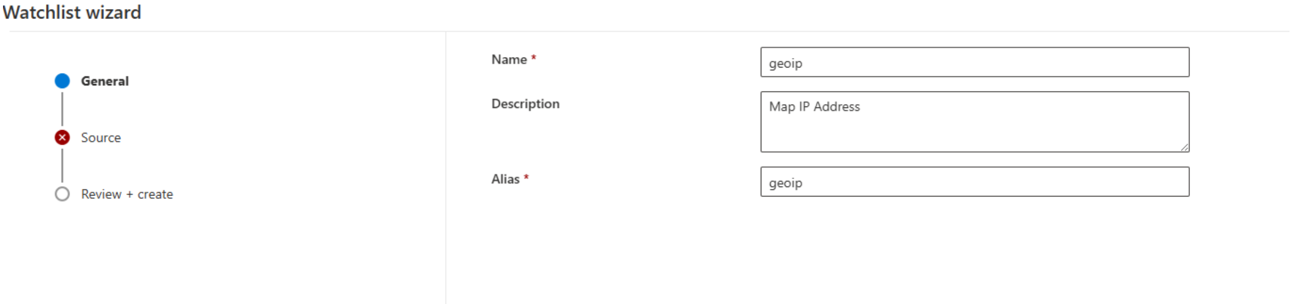
```
SecurityEvent
| where EventID == 4625
| where Account == "\\KANTIN"
| project TimeGenerated, IpAddress
```

imeGenerated [UTC] ↑↓	IpAddress
> 9/6/2025, 12:21:59.150 PM	185.156.73.62

Fig 34

Plotting the IP address on a Map

To plot the IP address of the general area these IPs are originating from, we need to create a Watchlist.
Click on the Sentinel instance, under configure, click on Watchlist


Watchlist wizard

Name * geoip

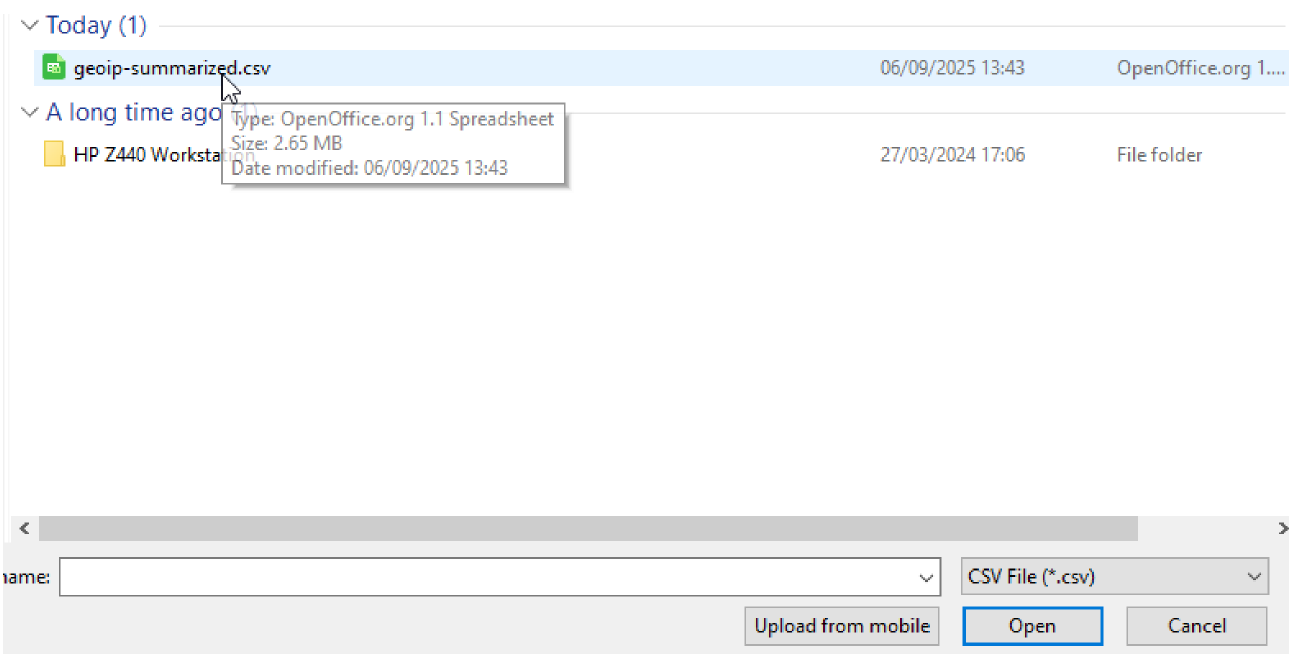
Description Map IP Address

Alias * geoip

Fig 35

Navigate to this GitHub, download the CSV file to your local device

https://raw.githubusercontent.com/joshmadakor1/lognpacific-public/refs/heads/main/misc/geoip-summarized.csv
The CSV file helps map the IP location of the



Today (1)

geoip-summarized.csv	06/09/2025 13:43	OpenOffice.org 1....

Type: OpenOffice.org 1.1 Spreadsheet
Size: 2.65 MB
Date modified: 06/09/2025 13:43

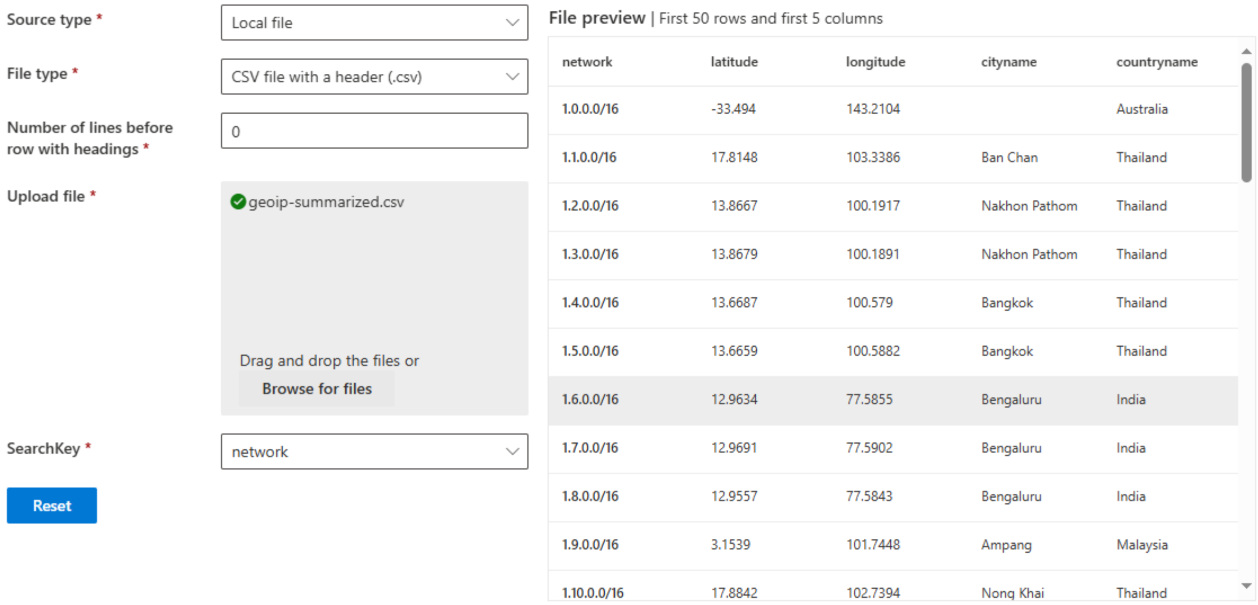
A long time ago (1)

HP Z440 Workstation	27/03/2024 17:06	File folder

name:

CSV File (*.csv)

Fig 36



Source type * Local file

File type * CSV file with a header (.csv)

Number of lines before row with headings * 0

Upload file * geoip-summarized.csv

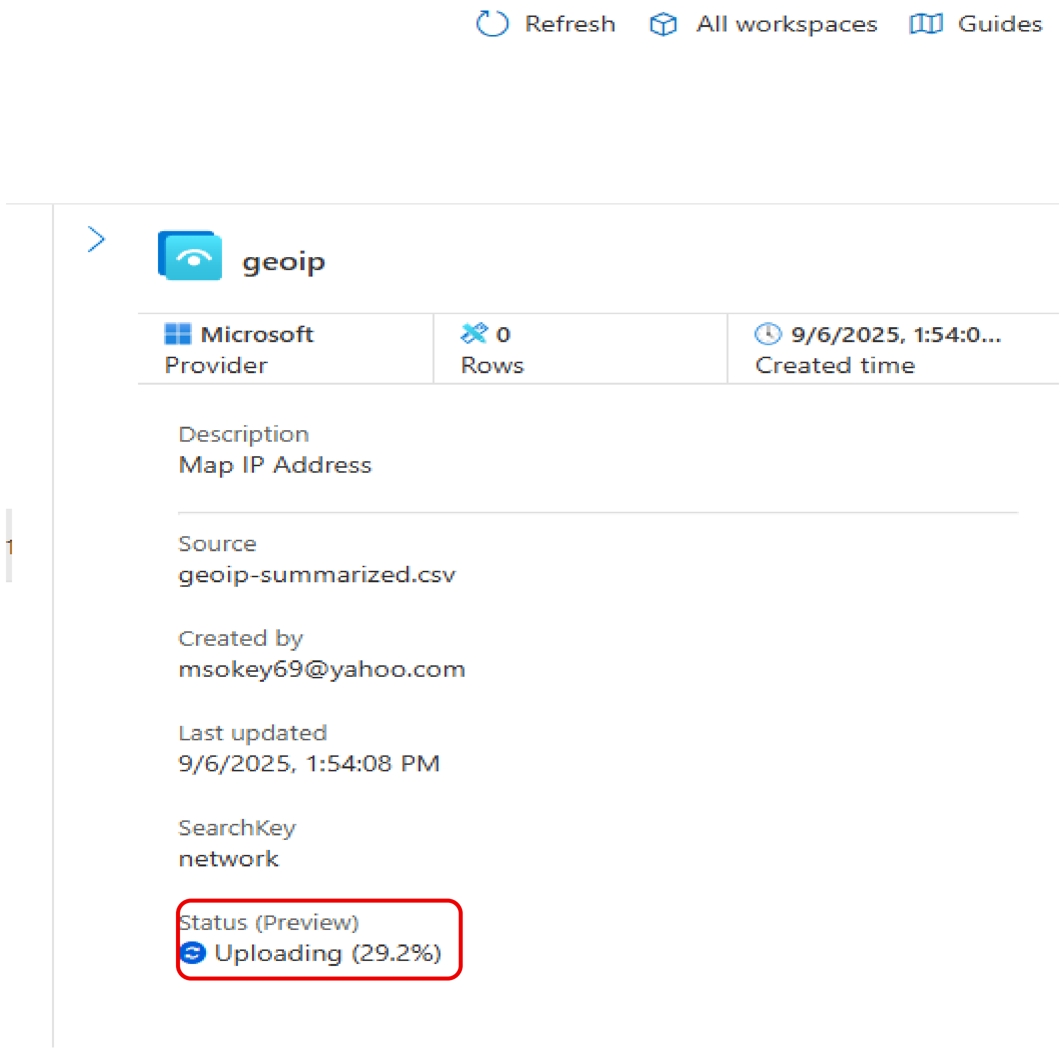
SearchKey * network

File preview | First 50 rows and first 5 columns

network	latitude	longitude	cityname	countryname
1.0.0.0/16	-33.494	143.2104		Australia
1.1.0.0/16	17.8148	103.3386	Ban Chan	Thailand
1.2.0.0/16	13.8667	100.1917	Nakhon Pathom	Thailand
1.3.0.0/16	13.8679	100.1891	Nakhon Pathom	Thailand
1.4.0.0/16	13.6687	100.579	Bangkok	Thailand
1.5.0.0/16	13.6659	100.5882	Bangkok	Thailand
1.6.0.0/16	12.9634	77.5855	Bengaluru	India
1.7.0.0/16	12.9691	77.5902	Bengaluru	India
1.8.0.0/16	12.9557	77.5843	Bengaluru	India
1.9.0.0/16	3.1539	101.7448	Ampang	Malaysia
1.10.0.0/16	17.8842	102.7394	Nong Khai	Thailand

Fig 37

In the watchlist, click on the geoip. Wait for the CSV to be ingested into azure



geoip

Microsoft
Provider

0
Rows

9/6/2025, 1:54:0...
Created time

Description
Map IP Address

Source
geoip-summarized.csv

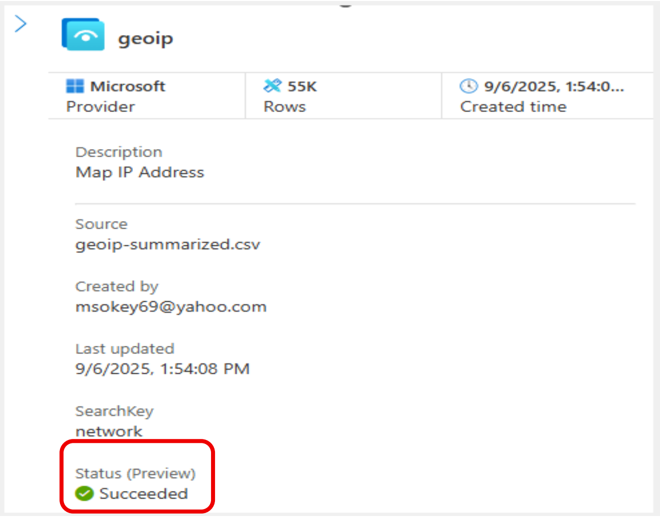
Created by
msokey69@yahoo.com

Last updated
9/6/2025, 1:54:08 PM

SearchKey
network

Status (Preview)
Uploading (29.2%)

Fig 38



geoip

Microsoft
Provider

55K
Rows

9/6/2025, 1:54:0...
Created time

Description
Map IP Address

Source
geoip-summarized.csv

Created by
msokey69@yahoo.com

Last updated
9/6/2025, 1:54:08 PM

SearchKey
network

Status (Preview)
Succeeded

Fig 39

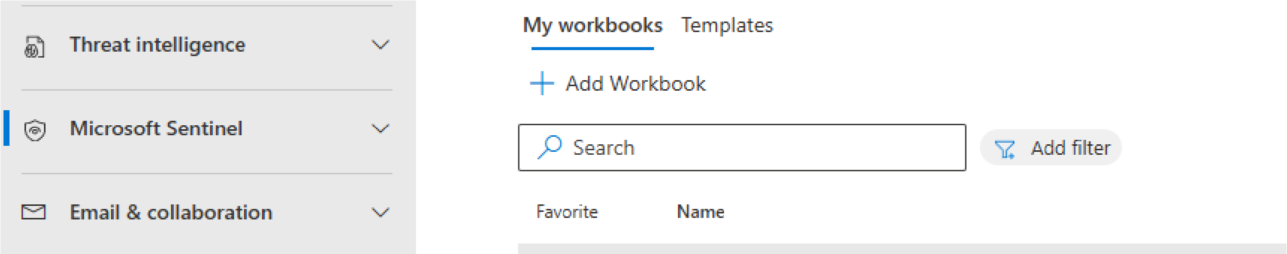
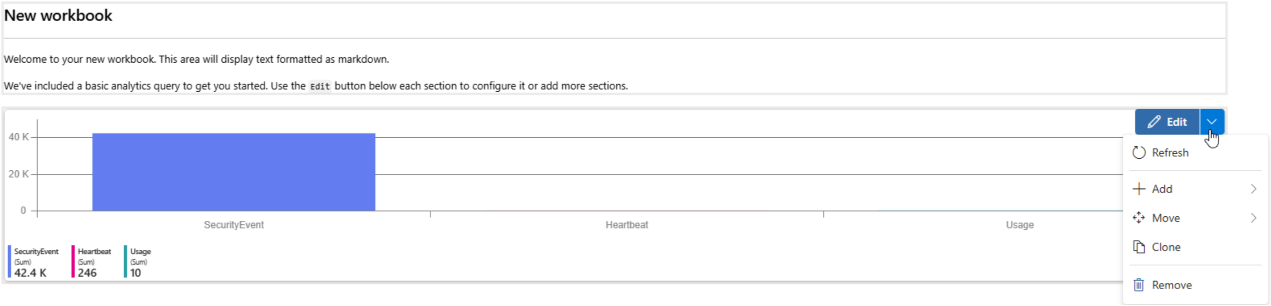


Fig 40

On the right hand side click on edit remove all the contents in the workbook.

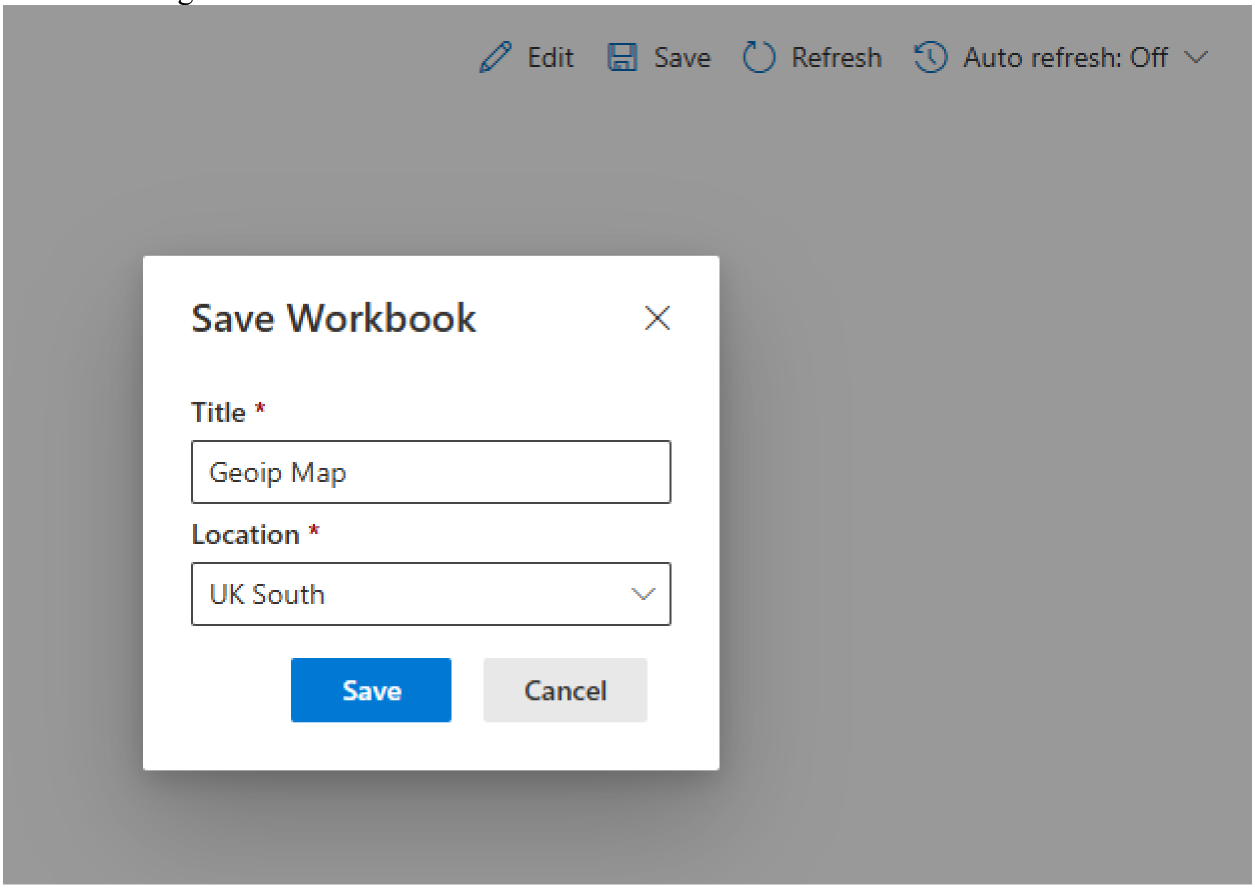

New workbook

Welcome to your new workbook. This area will display text formatted as markdown.

We've included a basic analytics query to get you started. Use the `Edit` button below each section to configure it or add more sections.

Fig 41

Click on Edit again Give the workbook a title and location. Click on save


Save Workbook

Title * Geoip Map

Location * UK South

Fig 42

Geoip Map

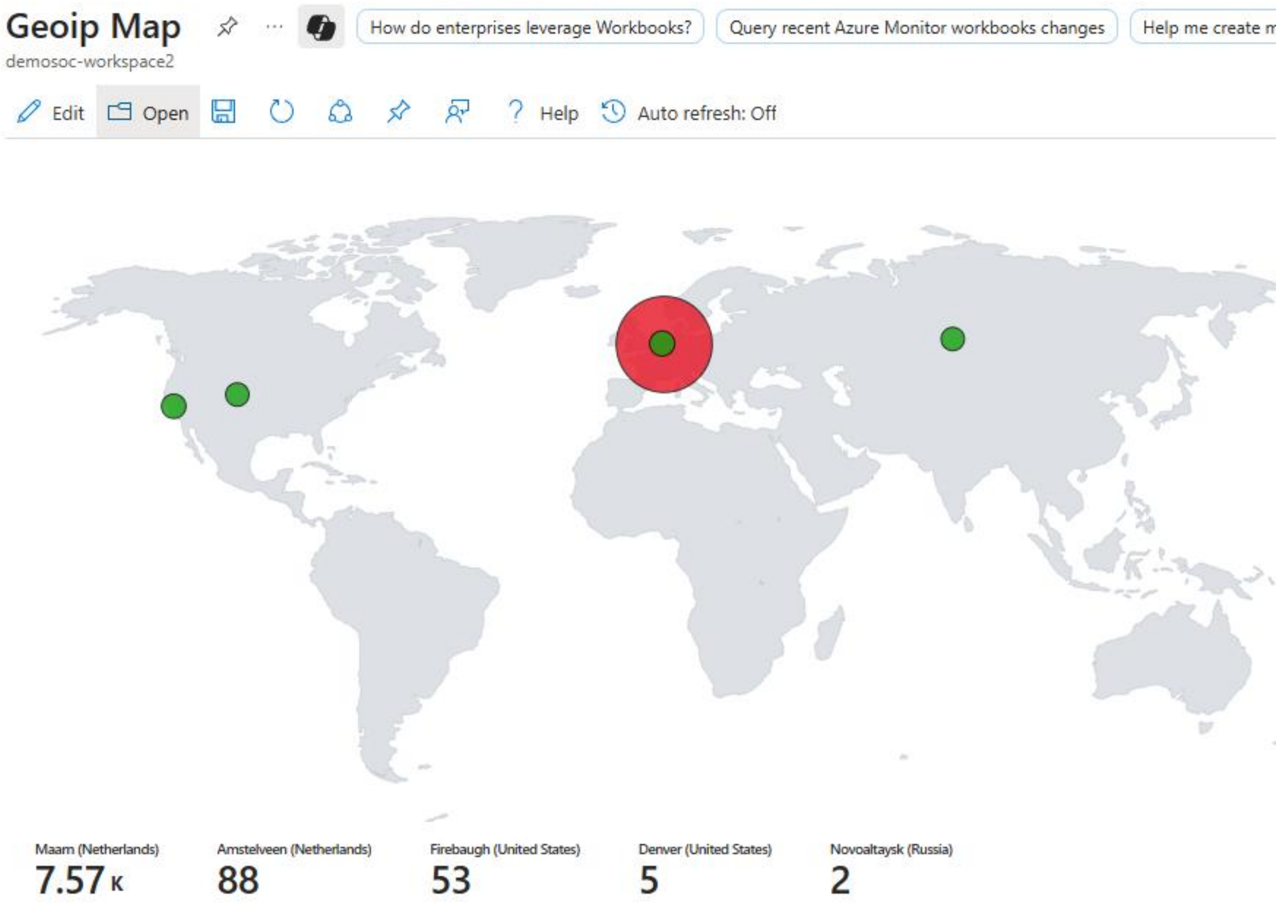
Open in Azure
Edit
Save
Save As

Click on Open in Azure. Click on edit. Select advanced query. Copy and paste the map.json contents.

Navigate to this website https://drive.google.com/file/d/1ErlVEK5cQjpGyOcu4T02xYy7F31dWuir/view?usp=drive_link and copy the map.json content to the advanced query and click done editing

```
{
        "type": 3,
        "content": {
        "version": "KqlItem/1.0",
        "query": "let GeoIPDB_FULL = _GetWatchlist(\"geoip\");\nlet
WindowsEvents = SecurityEvent;\nWindowsEvents | where EventID == 4625\n|
order by TimeGenerated desc\n| evaluate ipv4_lookup(GeoIPDB_FULL, IpAddress,
network)\n| summarize FailureCount = count() by IpAddress, latitude,
longitude, cityname, countryname\n| project FailureCount, AttackerIp =
IpAddress, latitude, longitude, city = cityname, country =
countryname,\nfriendly_location = strcat(cityname, \" (\", countryname,
\")\");",
        "size": 3,
        "timeContext": {
                "durationMs": 2592000000
        },
        "queryType": 0,
        "resourceType": "microsoft.operationalinsights/workspaces",
        "visualization": "map",
        "mapSettings": {
                "locInfo": "LatLong",
                "locInfoColumn": "countryname",
                "latitude": "latitude",
                "longitude": "longitude",
                "sizeSettings": "FailureCount",
                "sizeAggregation": "Sum",
                "opacity": 0.8,
                "labelSettings": "friendly_location",
                "legendMetric": "FailureCount",
                "legendAggregation": "Sum",
                "itemColorSettings": {
                "nodeColorField": "FailureCount",
                "colorAggregation": "Sum",
                "type": "heatmap",
                "heatmapPalette": "greenRed"
                }
        }
        },
        "name": "query - 0"
}
```

A map showing the general area from which the attacking Ips are originating will be displayed.


Geoip Map
demosoc-workspace2
How do enterprises leverage Workbooks?
Query recent Azure Monitor workbooks changes
Help me create m
Edit
Open
Help
Auto refresh: Off

Maam (Netherlands)	Amstelveen (Netherlands)	Firebaugh (United States)	Denver (United States)	Novoaltaysk (Russia)
7.57 K	88	53	5	2

Fig 43

To get a variety of results, the VM needs to run for a period of time of more than 24 hrs at least.

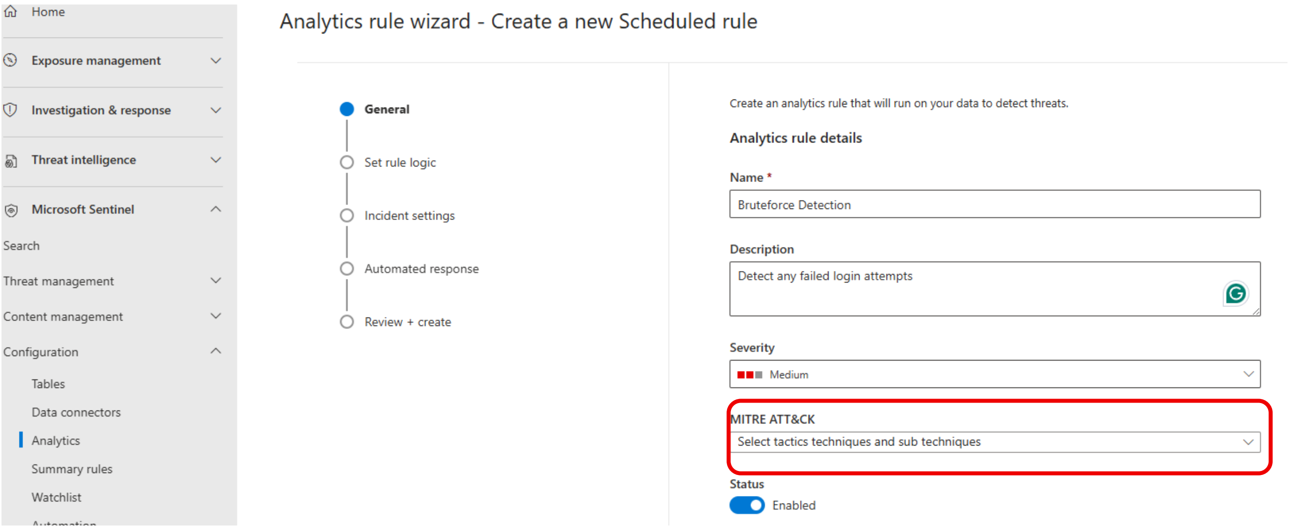
With the results obtained, we can create an incident rule that will generate an alert. For the SOC to investigate and resolve.

To achieve this, we need to create a scheduled rule that will run, interrogate the logs, compare them to the rule, and if anything fails, an alert is generated.

On the Sentinel page, click on configuration. The new Sentinel page will direct you to the Microsoft Defender page. Under configuration, click on Analytics

Create a Scheduled Query.

Navigate to the analytics tab



Analytics rule wizard - Create a new Scheduled rule

Create an analytics rule that will run on your data to detect threats.

Analytics rule details

Name *: Bruteforce Detection

Description: Detect any failed login attempts

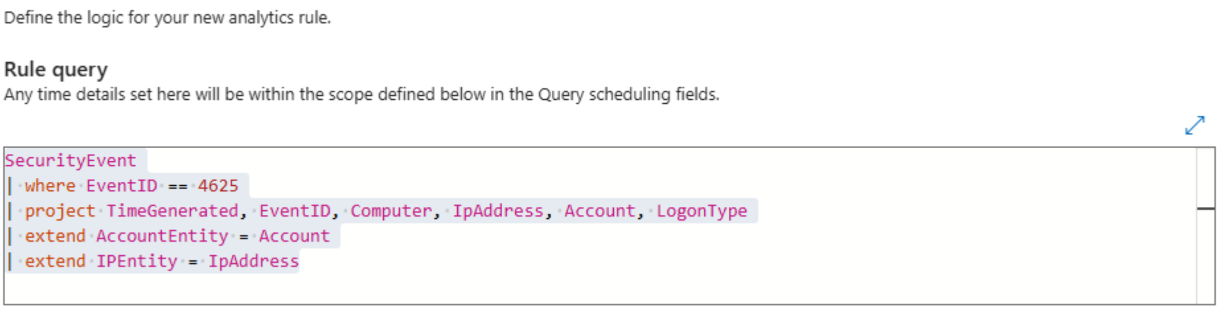
Severity: Medium

MITRE ATT&CK: Select tactics techniques and sub techniques

Status: Enabled

Fig 44

Write the query that will determine if the rule has been violated by the event in the logs.



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.

```
SecurityEvent
| where EventID == 4625
| project TimeGenerated, EventID, Computer, IpAddress, Account, LogonType
| extend AccountEntity = Account
| extend IPEntity = IpAddress
```

Fig 45

Query Explained

SecurityEvent

- This specifies the table you're querying.
- In Azure Log Analytics, SecurityEvent contains Windows security event logs.
- These include things like logon attempts, privilege use, account management, etc.

| where EventID == 4625

- Filters the data to only include rows (events) where EventID is 4625.
- 4625 is the Windows Event ID for a failed logon attempt (due to a bad password, unknown user, etc.).

| project TimeGenarated, EventID, Computer, IpAddress, Account, LogonType

- This selects (projects) only the specific columns you want to see in the results:
  - TimeGenerated: When the event was logged.

  - EventID: Should be 4625 in every row.
  - Computer: Name of the machine where the event was logged.
  - IpAddress: IP address from where the login was attempted.
  - Account: The user account name used in the attempt.
  - LogonType: Indicates the type of logon (e.g., interactive, remote, network).

| extend AccountEntity = Account

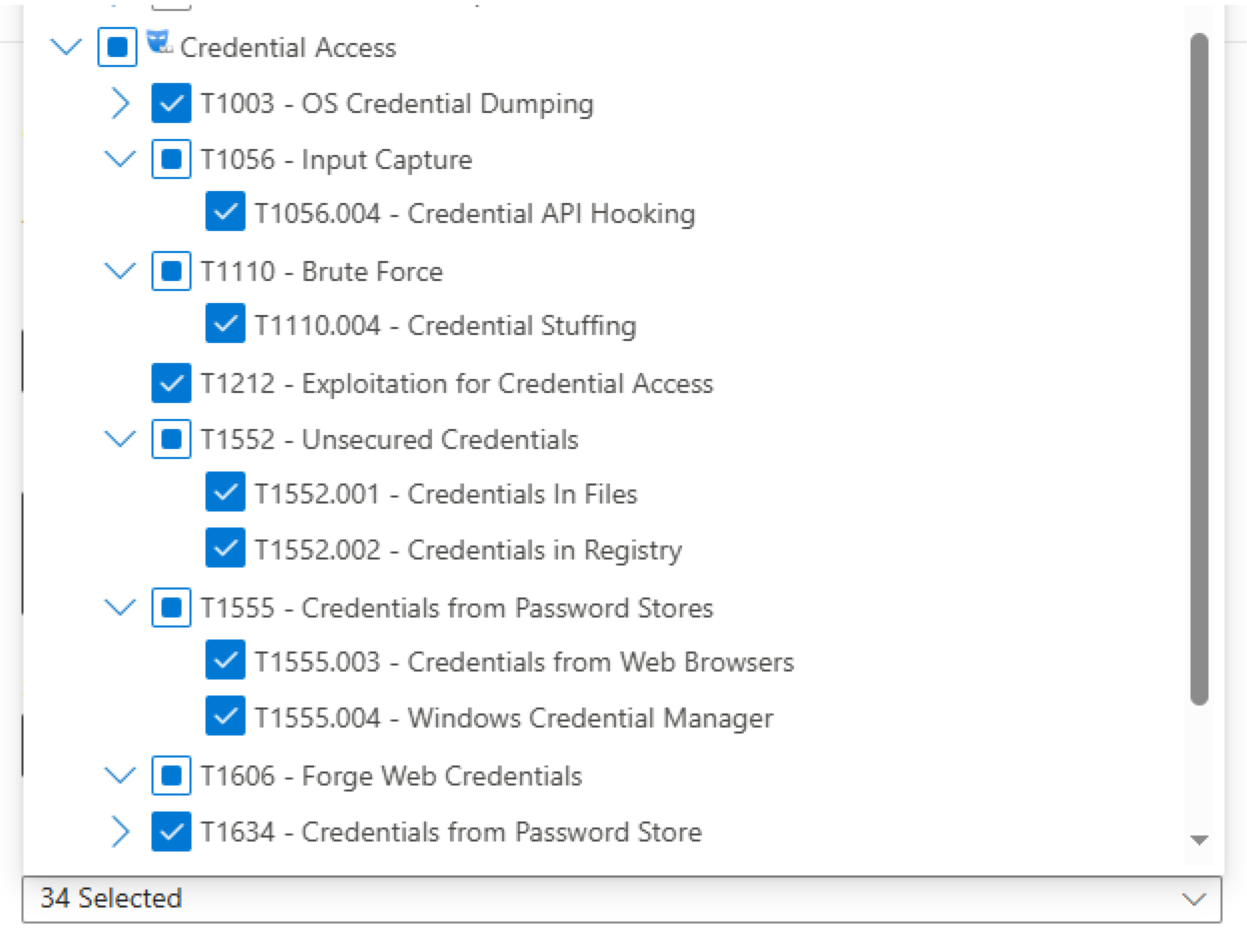
- Creates a new column called AccountEntity and copies the value from the Account column into it.
- This is often done for entity mapping in Microsoft Sentinel, where AccountEntity can be linked to identity analytics.

| extend IPEntity = IpAddress

- Similar to the above: creates a new column IPEntity with the same values as IpAddress.

This is for linking with network entity analytics, IP investigations, etc.

In the set rule logic, under the MITRE attack section, see fig 44, select the tactics, techniques, and sub-techniques. See fig 44

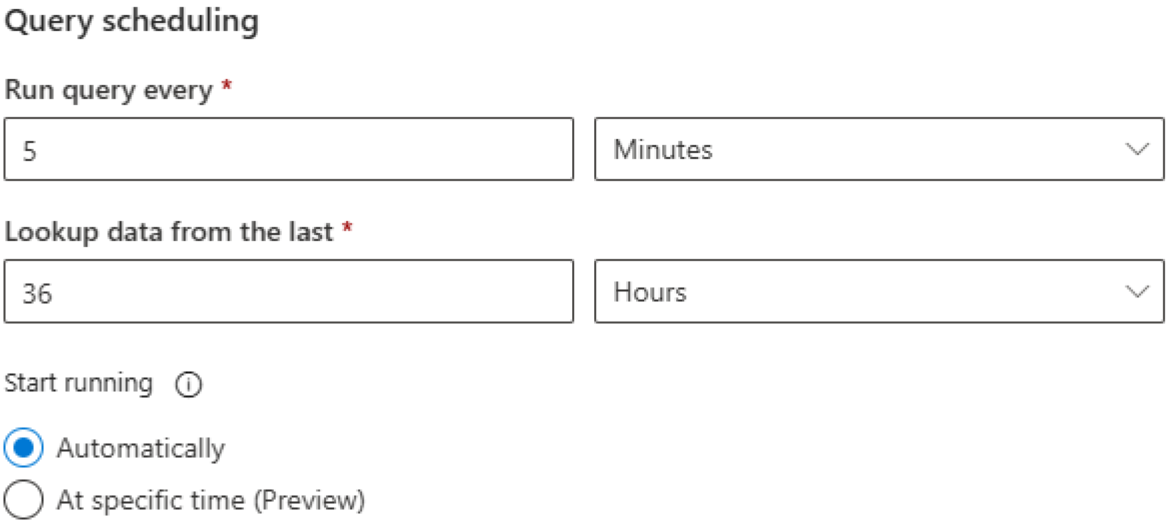


- ■ Credential Access
  - ☑ T1003 - OS Credential Dumping
  - ■ T1056 - Input Capture
    - ☑ T1056.004 - Credential API Hooking
  - ■ T1110 - Brute Force
    - ☑ T1110.004 - Credential Stuffing
  - ☑ T1212 - Exploitation for Credential Access
  - ■ T1552 - Unsecured Credentials
    - ☑ T1552.001 - Credentials In Files
    - ☑ T1552.002 - Credentials in Registry
  - ■ T1555 - Credentials from Password Stores
    - ☑ T1555.003 - Credentials from Web Browsers
    - ☑ T1555.004 - Windows Credential Manager
  - ■ T1606 - Forge Web Credentials
  - ☑ T1634 - Credentials from Password Store

34 Selected

Fig 46

Set how often the rule will run.



Query scheduling

Run query every *: 5 Minutes

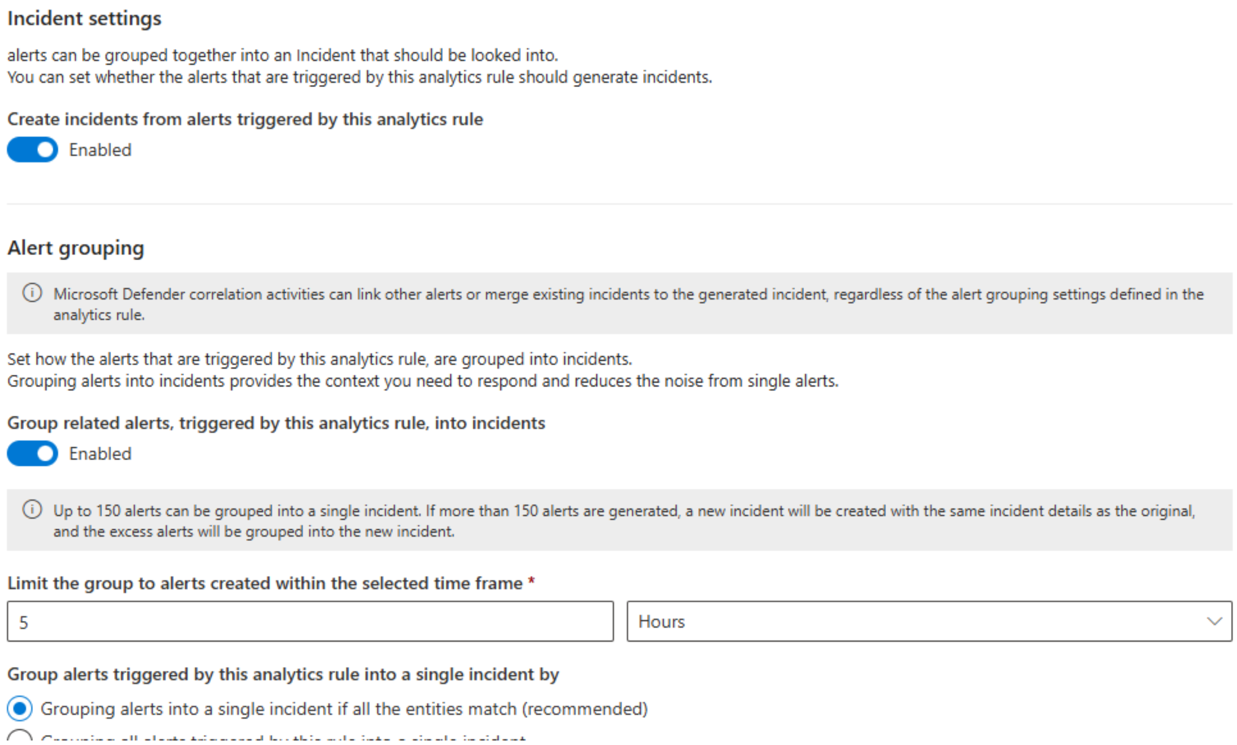
Lookup data from the last *: 36 Hours

Start running ⓘ

● Automatically

○ At specific time (Preview)

Fig 47



Incident settings

alerts can be grouped together into an Incident that should be looked into.
You can set whether the alerts that are triggered by this analytics rule should generate incidents.

Create incidents from alerts triggered by this analytics rule

Enabled

Alert grouping

ⓘ Microsoft Defender correlation activities can link other alerts or merge existing incidents to the generated incident, regardless of the alert grouping settings defined in the analytics rule.

Set how the alerts that are triggered by this analytics rule, are grouped into incidents.
Grouping alerts into incidents provides the context you need to respond and reduces the noise from single alerts.

Group related alerts, triggered by this analytics rule, into incidents

Enabled

ⓘ Up to 150 alerts can be grouped into a single incident. If more than 150 alerts are generated, a new incident will be created with the same incident details as the original, and the excess alerts will be grouped into the new incident.

Limit the group to alerts created within the selected time frame *

5 | Hours

Group alerts triggered by this analytics rule into a single incident by

● Grouping alerts into a single incident if all the entities match (recommended)

○ Grouping all alerts triggered by this rule into a single incident

Fig 48

Enable Alert grouping

After a while, an Incident will be created

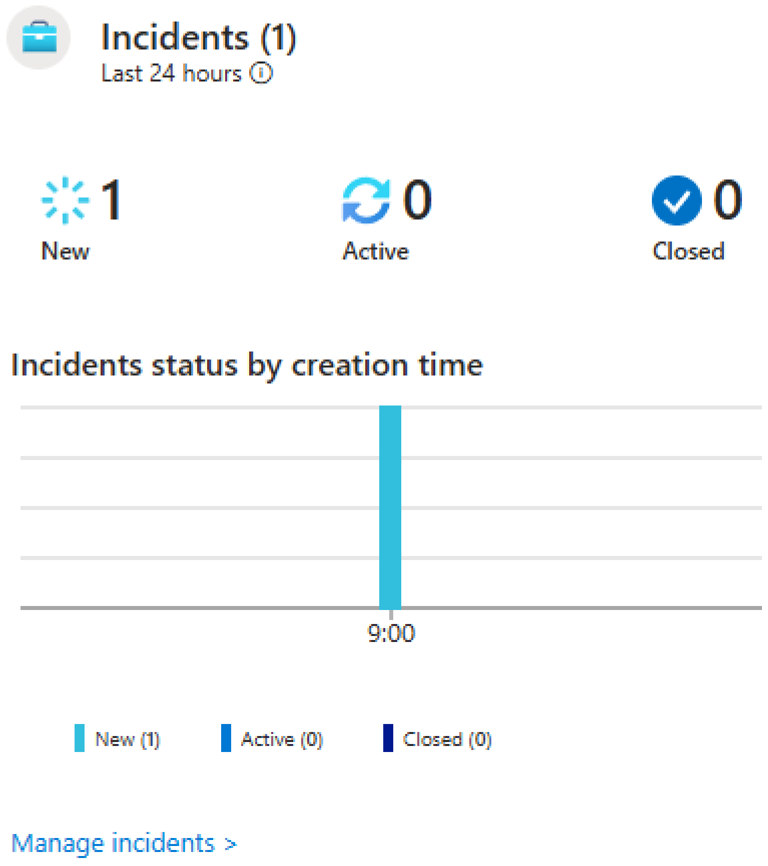
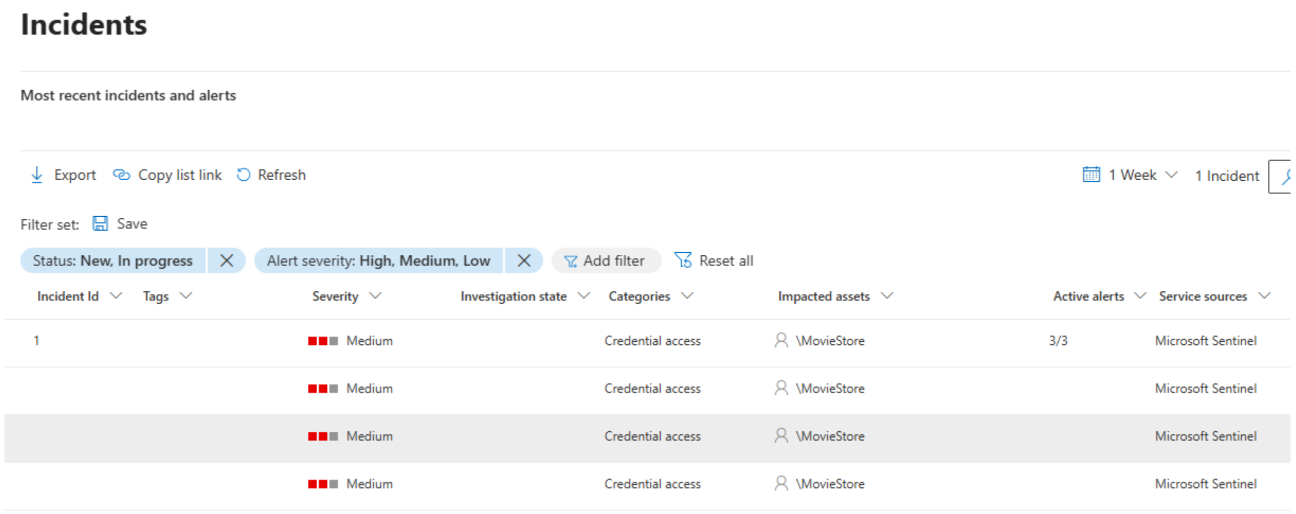


Fig 49



Incidents

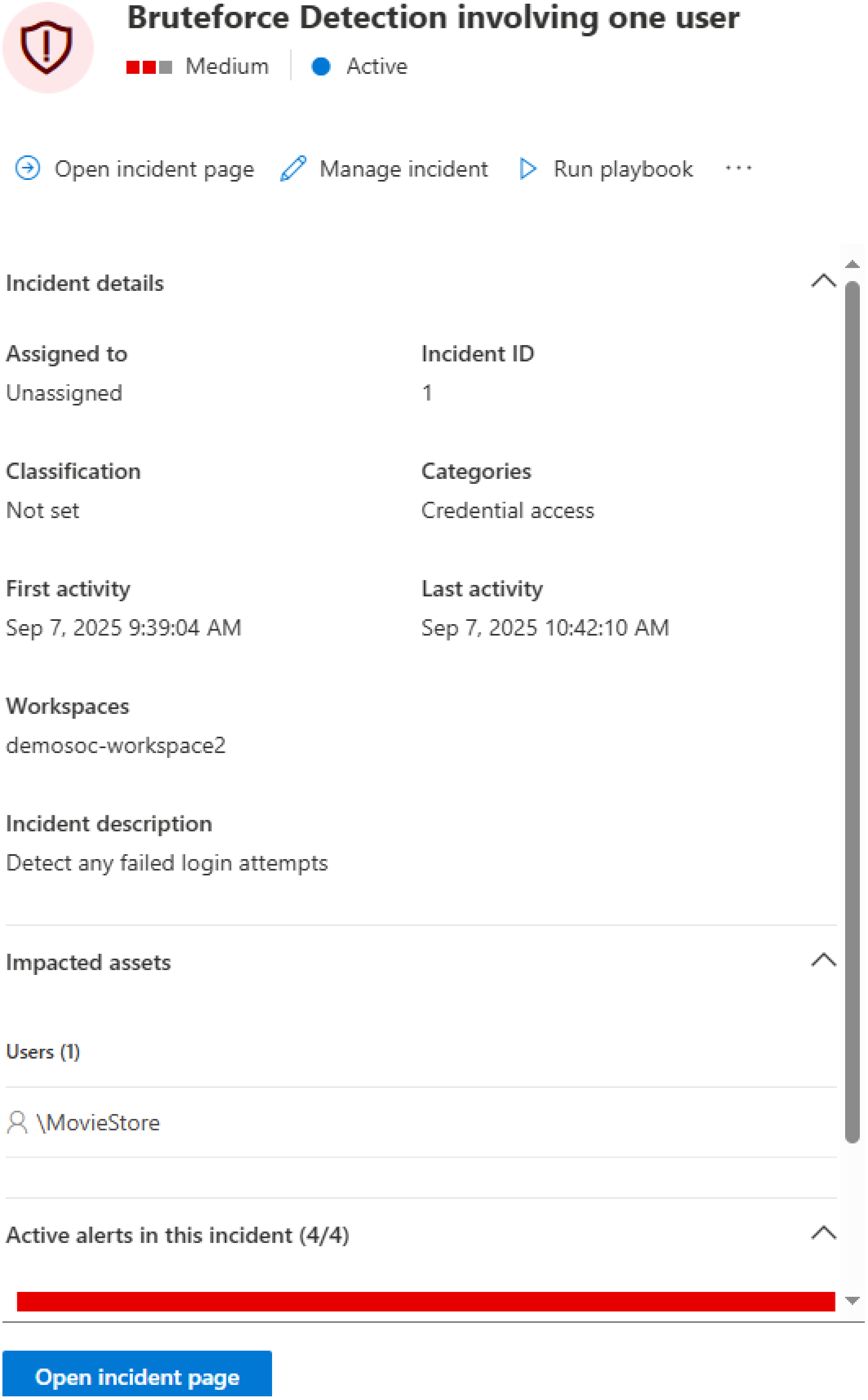
Most recent incidents and alerts

Status: **New, In progress**

Alert severity: **High, Medium, Low**

Incident Id	Tags	Severity	Investigation state	Categories	Impacted assets	Active alerts	Service sources
1		■■■ Medium		Credential access	\MovieStore	3/3	Microsoft Sentinel
		■■■ Medium		Credential access	\MovieStore		Microsoft Sentinel
		■■■ Medium		Credential access	\MovieStore		Microsoft Sentinel
		■■■ Medium		Credential access	\MovieStore		Microsoft Sentinel

Fig 50



Bruteforce Detection involving one user

Medium | ● Active

Open incident page   Manage incident   Run playbook   ···

Incident details

Assigned to
Unassigned

Incident ID
1

Classification
Not set

Categories
Credential access

First activity
Sep 7, 2025 9:39:04 AM

Last activity
Sep 7, 2025 10:42:10 AM

Workspaces
demosoc-workspace2

Incident description
Detect any failed login attempts

Impacted assets

Users (1)

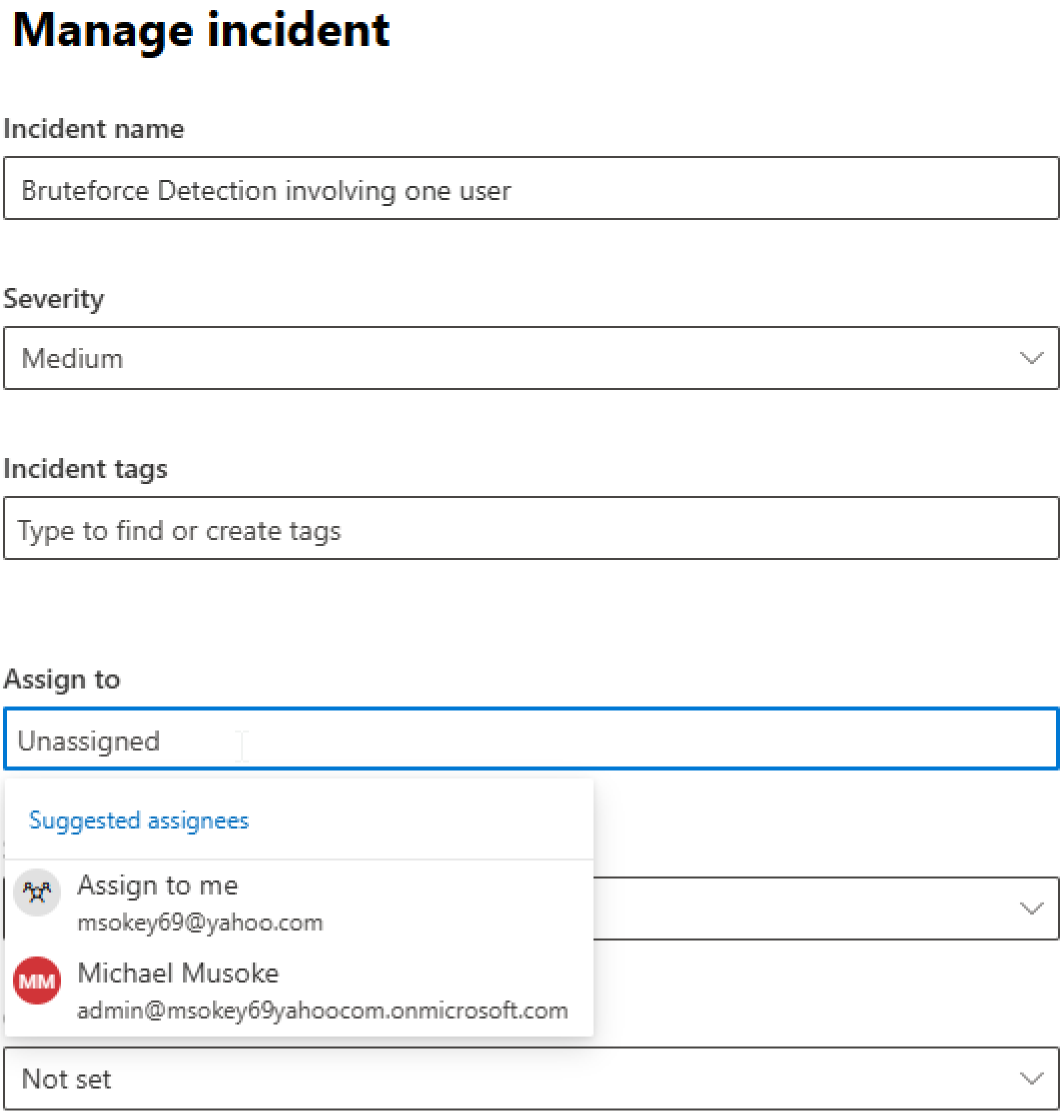
\MovieStore

Active alerts in this incident (4/4)

Open incident page

Fig 51

Click on the Open Incident page, see fig 51 to manage the indent. Assign the incident to one of the Analysts.



Manage incident

Incident name: Bruteforce Detection involving one user

Severity: Medium

Incident tags: Type to find or create tags

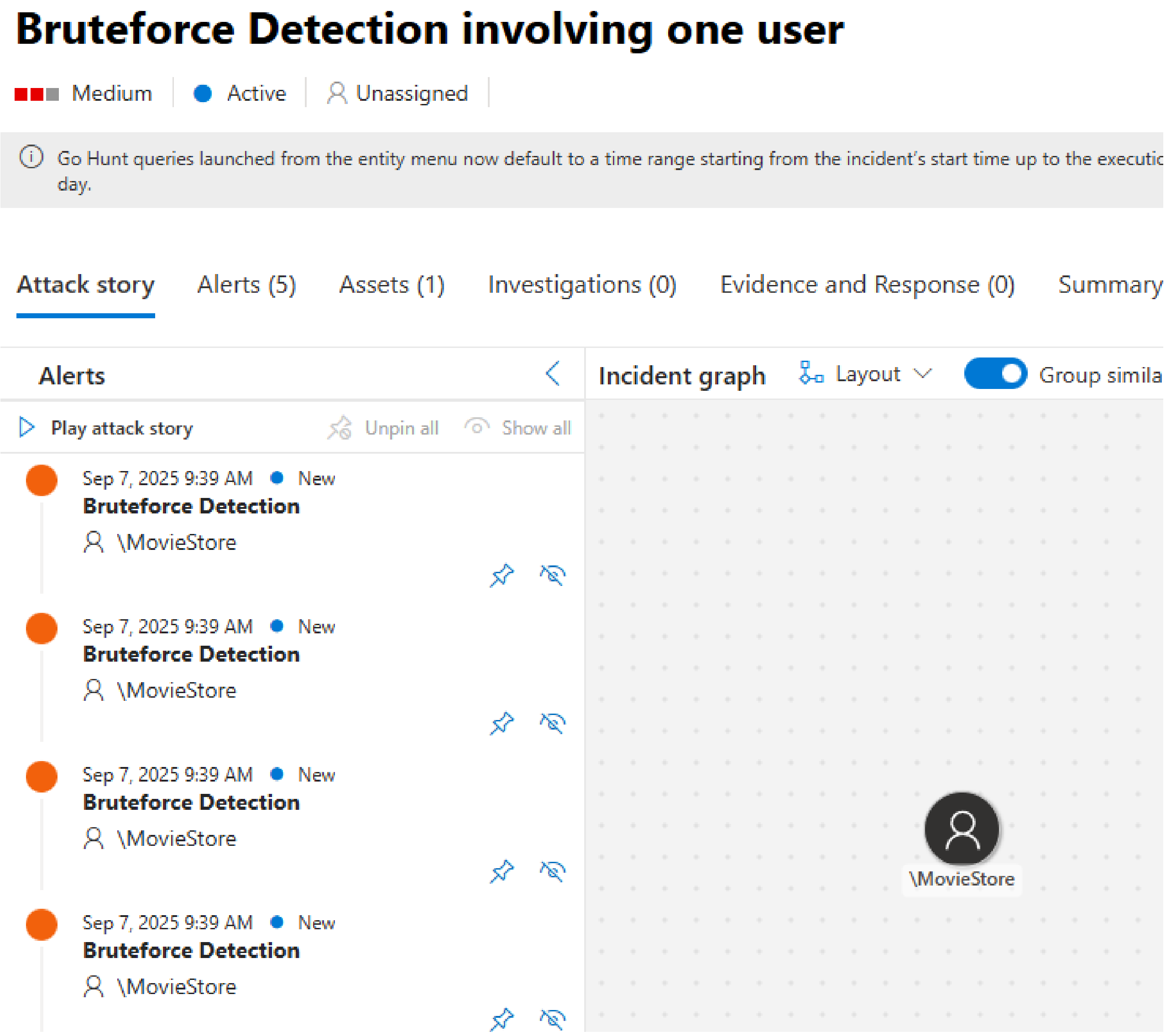
Assign to: Unassigned

Suggested assignees

- Assign to me
  msokey69@yahoo.com
- Michael Musoke
  admin@msokey69yahoocom.onmicrosoft.com

Not set

Fig 52



Bruteforce Detection involving one user

Medium | Active | Unassigned

Go Hunt queries launched from the entity menu now default to a time range starting from the incident's start time up to the executic day.

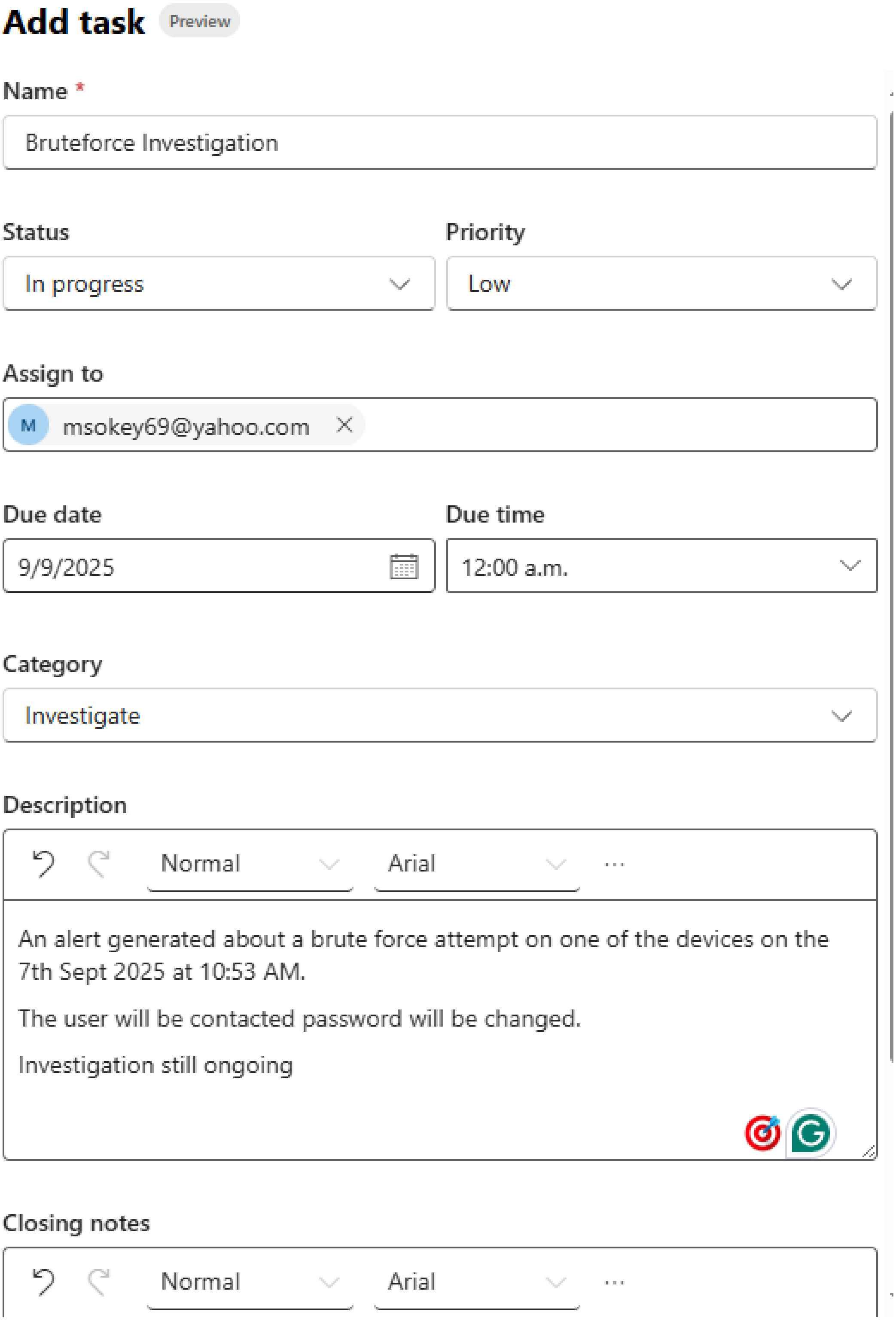
Sep 7, 2025 9:39 AM ● New
Bruteforce Detection
\MovieStore

Sep 7, 2025 9:39 AM ● New
Bruteforce Detection
\MovieStore

Sep 7, 2025 9:39 AM ● New
Bruteforce Detection
\MovieStore

Sep 7, 2025 9:39 AM ● New
Bruteforce Detection
\MovieStore

Fig 54



Add task

Name *

Bruteforce Investigation

Status

In progress

Priority

Low

Assign to

M msokey69@yahoo.com

Due date

9/9/2025

Due time

12:00 a.m.

Category

Investigate

Description

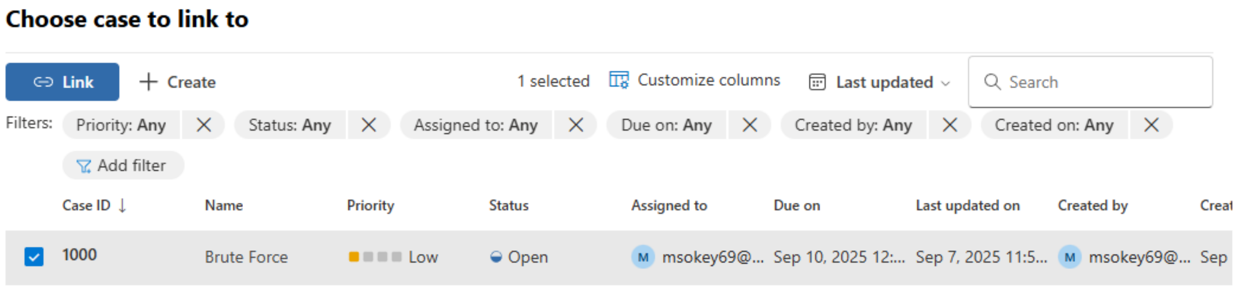
An alert generated about a brute force attempt on one of the devices on the 7th Sept 2025 at 10:53 AM.

The user will be contacted password will be changed.

Investigation still ongoing

Closing notes

Fig 55



Choose case to link to

Filters: Priority: Any | Status: Any | Assigned to: Any | Due on: Any | Created by: Any | Created on: Any

	Case ID ↓	Name	Priority	Status	Assigned to	Due on	Last updated on	Created by	Creat
☑	1000	Brute Force	Low	Open	msokey69@...	Sep 10, 2025 12:...	Sep 7, 2025 11:5...	msokey69@...	Sep

Fig 56

The analyst will investigate the incident to completion and resolve the incident giving a brief report of what was done. If the incident needs to be escalated, then the analyst will include reasons why otherwise, the case can be closed.

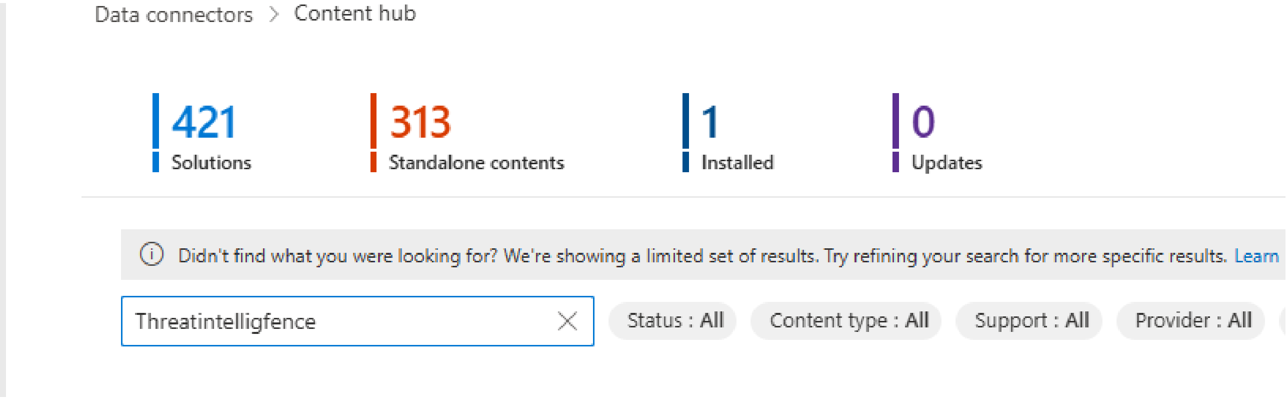
Threat Intelligence

Threat Intelligence (TI) refers to the collection, analysis, and application of data about existing and emerging threats. This includes information on malicious IP addresses, domains, malware hashes, attack techniques, and threat actor behavior. The goal of threat intelligence is to provide actionable insights that help security teams anticipate, identify, and respond to cyber threats more effectively. In the context of a Security Operations Center (SOC), threat intelligence is a critical capability for the following reasons:

1. **Enhanced Detection Accuracy**
   By enriching alerts and logs with threat intelligence feeds, SOC analysts can determine whether suspicious activity is linked to known malicious actors or infrastructure. This reduces false positives and ensures alerts carry meaningful context.
2. **Proactive Defense**
   Threat intelligence allows SOCs to stay ahead of attackers by identifying emerging tactics, techniques, and procedures (TTPs) based on frameworks such as MITRE ATT&CK. This enables proactive measures before an attack fully develops.
3. **Faster Incident Response**
   When an incident occurs, threat intelligence provides context about indicators of compromise (IoCs), helping analysts quickly prioritize and respond to critical threats. For example, knowing that an IP address is part of a botnet can speed up containment decisions.
4. **Strategic Insights**
   Beyond day-to-day detection, threat intelligence informs long-term security strategy by highlighting adversary groups targeting the industry, common attack vectors, and gaps in the organization’s defenses.
5. **Integration with SOC Tools**
   Modern SIEM and SOAR platforms like Microsoft Sentinel and Microsoft Defender XDR integrate directly with threat intelligence sources (e.g., Pulsedive, MISP). This seamless integration ensures that real-time threat data strengthens automated detection, hunting, and response capabilities.

Ingesting Pulsedive Data

Under Data connectors, select Content hub and search for Threatintelligence


Data connectors > Content hub

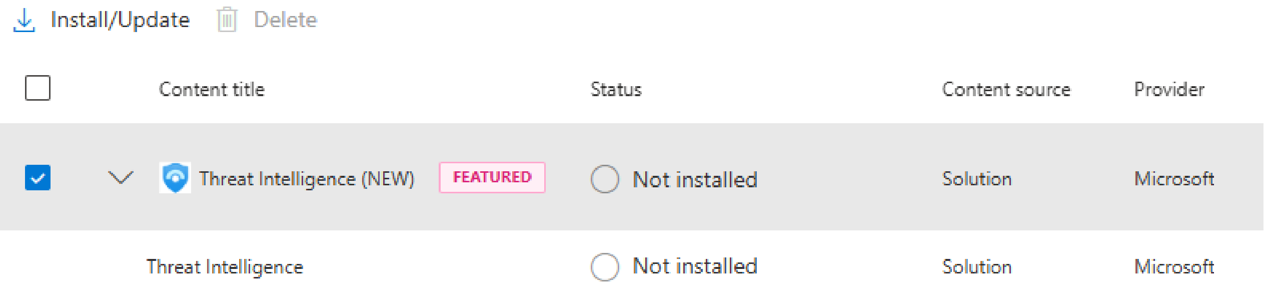
421 Solutions
313 Standalone contents
1 Installed
0 Updates

ⓘ Didn't find what you were looking for? We're showing a limited set of results. Try refining your search for more specific results. Learn

Threatintelligfence

Fig 57

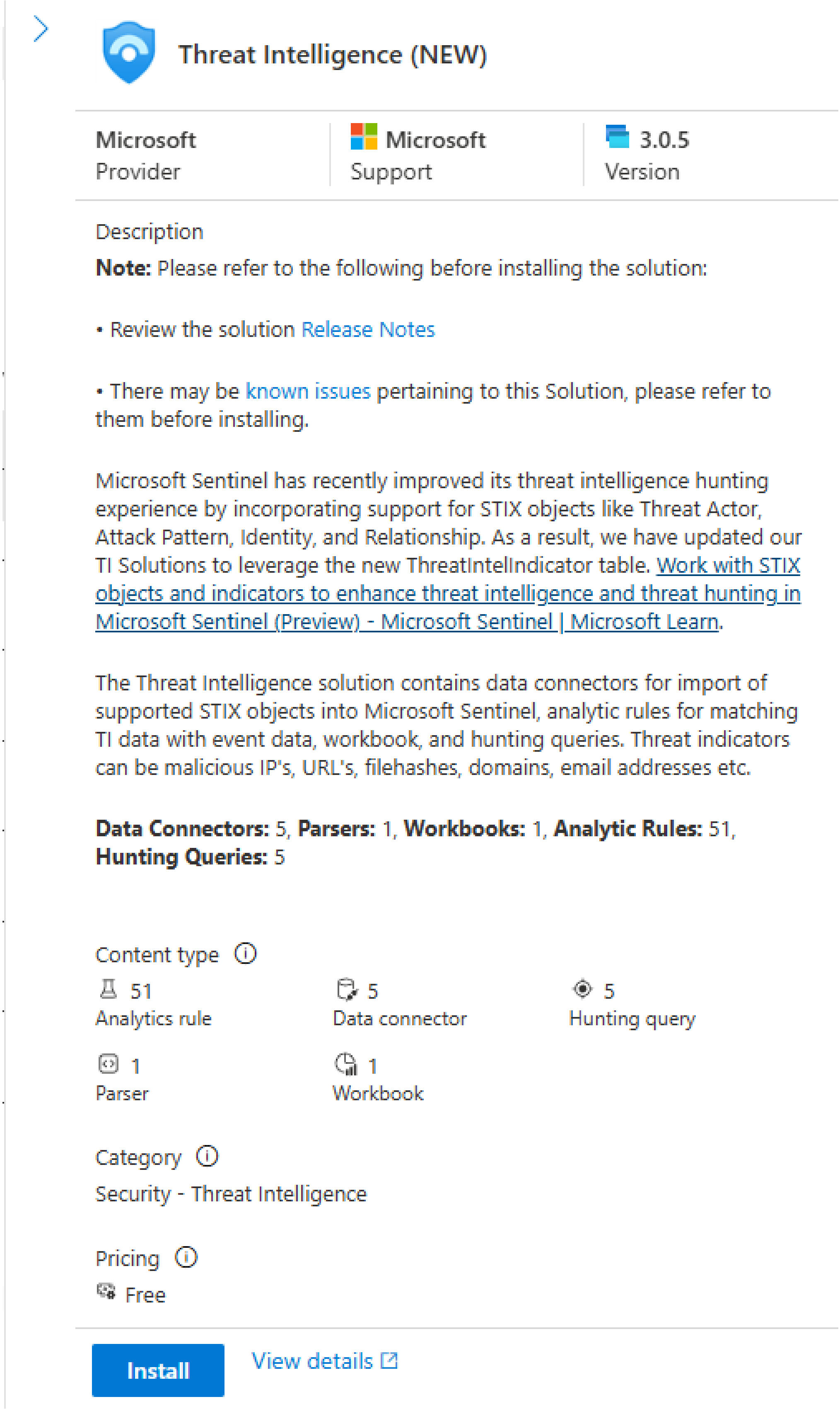
Select the first instance of Threat Intelligence



□	Content title	Status	Content source	Provider
☑	Threat Intelligence (NEW) FEATURED	○ Not installed	Solution	Microsoft
	Threat Intelligence	○ Not installed	Solution	Microsoft

Fig 58

On the right-hand side of the screen, click on Install for the connector to be installed



Threat Intelligence (NEW)

Microsoft
Provider

Microsoft
Support

3.0.5
Version

Description

Note: Please refer to the following before installing the solution:

• Review the solution Release Notes

• There may be known issues pertaining to this Solution, please refer to them before installing.

Microsoft Sentinel has recently improved its threat intelligence hunting experience by incorporating support for STIX objects like Threat Actor, Attack Pattern, Identity, and Relationship. As a result, we have updated our TI Solutions to leverage the new ThreatIntelIndicator table. Work with STIX objects and indicators to enhance threat intelligence and threat hunting in Microsoft Sentinel (Preview) - Microsoft Sentinel | Microsoft Learn.

The Threat Intelligence solution contains data connectors for import of supported STIX objects into Microsoft Sentinel, analytic rules for matching TI data with event data, workbook, and hunting queries. Threat indicators can be malicious IP's, URL's, filehashes, domains, email addresses etc.

Data Connectors: 5, **Parsers:** 1, **Workbooks:** 1, **Analytic Rules:** 51, **Hunting Queries:** 5

Content type

51 Analytics rule

5 Data connector

5 Hunting query

1 Parser

1 Workbook

Category

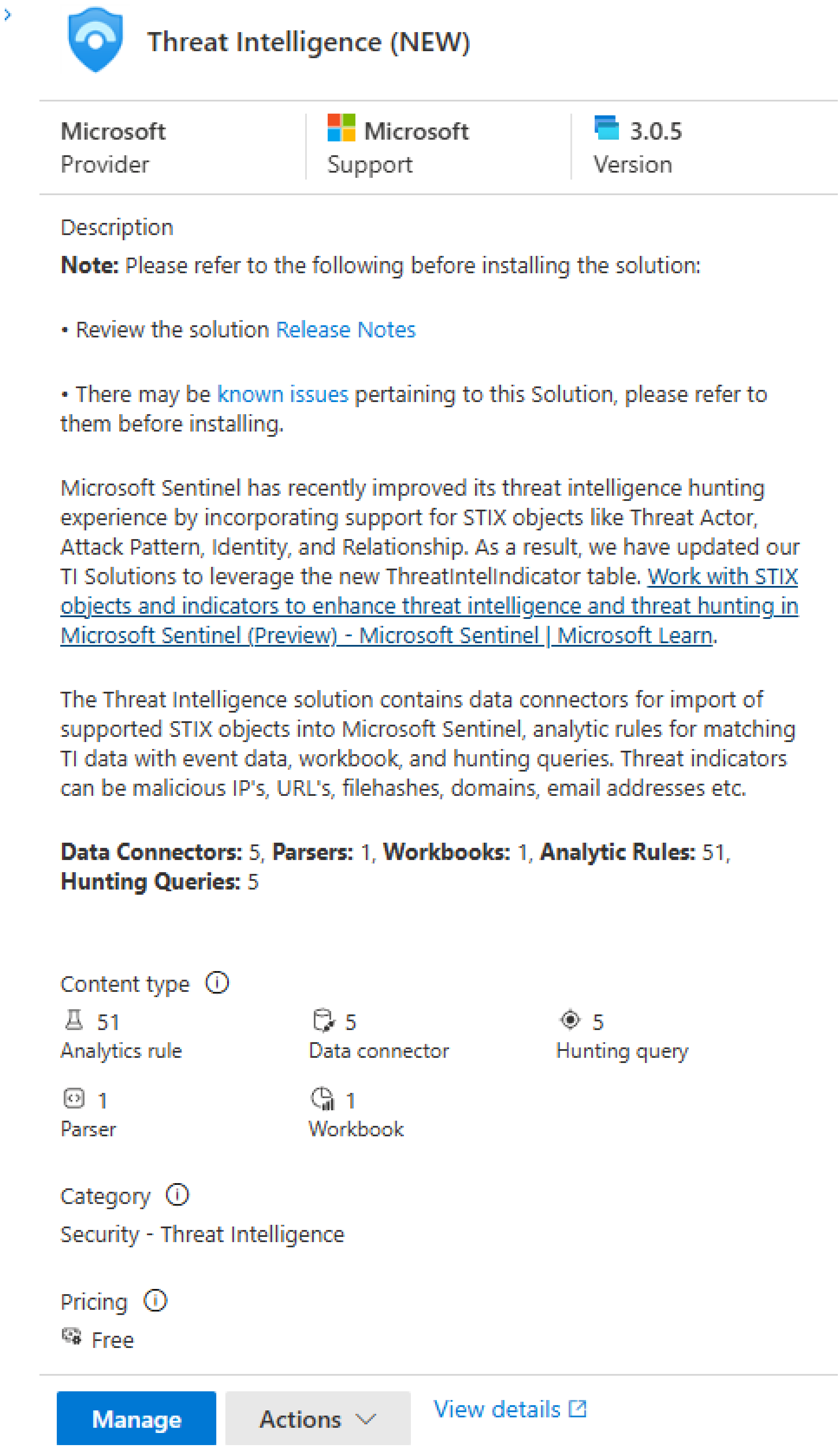
Security - Threat Intelligence

Pricing

Free

Fig 59

Click on Manage after the installation is completed



Threat Intelligence (NEW)

Microsoft
Provider

Microsoft
Support

3.0.5
Version

Description

Note: Please refer to the following before installing the solution:

• Review the solution Release Notes

• There may be known issues pertaining to this Solution, please refer to them before installing.

Microsoft Sentinel has recently improved its threat intelligence hunting experience by incorporating support for STIX objects like Threat Actor, Attack Pattern, Identity, and Relationship. As a result, we have updated our TI Solutions to leverage the new ThreatIntelIndicator table. Work with STIX objects and indicators to enhance threat intelligence and threat hunting in Microsoft Sentinel (Preview) - Microsoft Sentinel | Microsoft Learn.

The Threat Intelligence solution contains data connectors for import of supported STIX objects into Microsoft Sentinel, analytic rules for matching TI data with event data, workbook, and hunting queries. Threat indicators can be malicious IP's, URL's, filehashes, domains, email addresses etc.

Data Connectors: 5, **Parsers:** 1, **Workbooks:** 1, **Analytic Rules:** 51, **Hunting Queries:** 5

Content type

51 Analytics rule

5 Data connector

5 Hunting query

1 Parser

1 Workbook

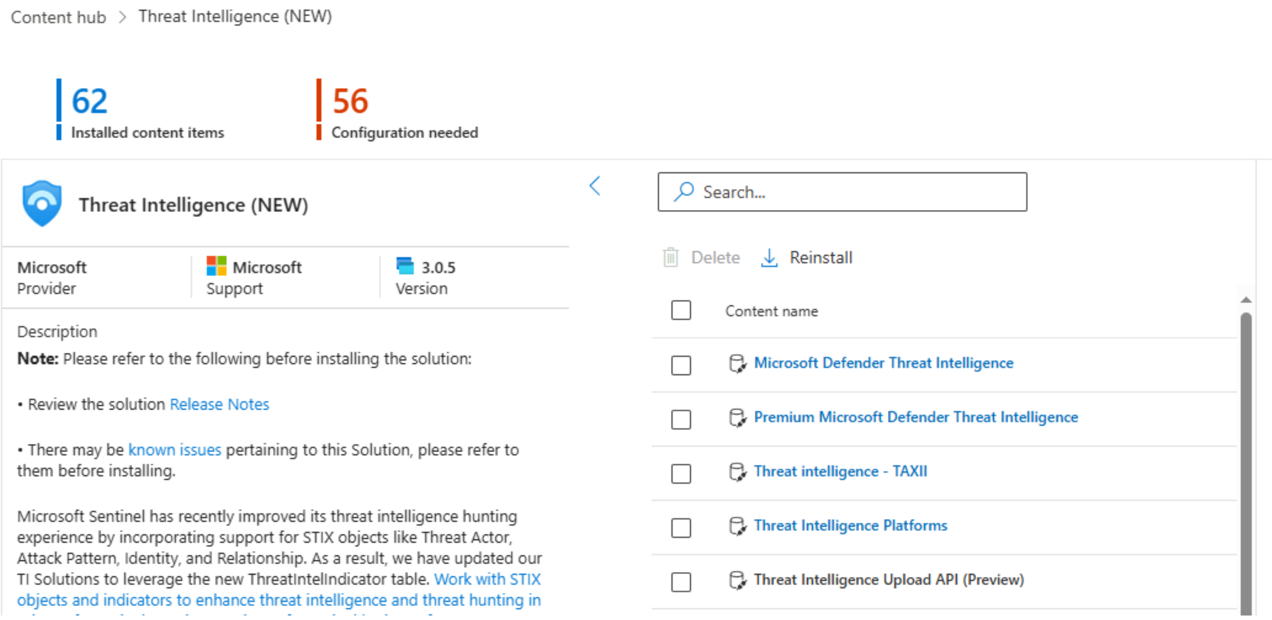
Category

Security - Threat Intelligence

Pricing

Free

Fig 60



Content hub > Threat Intelligence (NEW)

62 Installed content items

56 Configuration needed

Threat Intelligence (NEW)

Microsoft
Provider

Microsoft
Support

3.0.5
Version

Description

Note: Please refer to the following before installing the solution:

• Review the solution Release Notes

• There may be known issues pertaining to this Solution, please refer to them before installing.

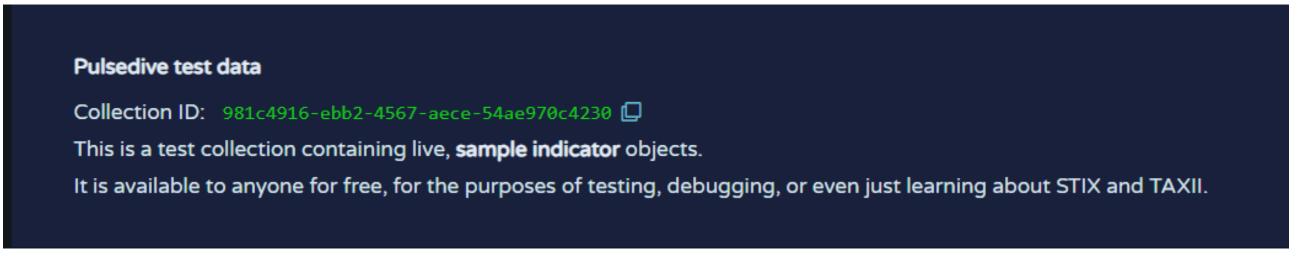
Microsoft Sentinel has recently improved its threat intelligence hunting experience by incorporating support for STIX objects like Threat Actor, Attack Pattern, Identity, and Relationship. As a result, we have updated our TI Solutions to leverage the new ThreatIntelIndicator table. Work with STIX objects and indicators to enhance threat intelligence and threat hunting in

☐	Content name
☐	Microsoft Defender Threat Intelligence
☐	Premium Microsoft Defender Threat Intelligence
☐	Threat intelligence - TAXII
☐	Threat Intelligence Platforms
☐	Threat Intelligence Upload API (Preview)

Fig 61

On a new web page, open an account with Pulsedive. Threat Intelligence - Pulsedive

To receive data from Pulsedive an account is required.



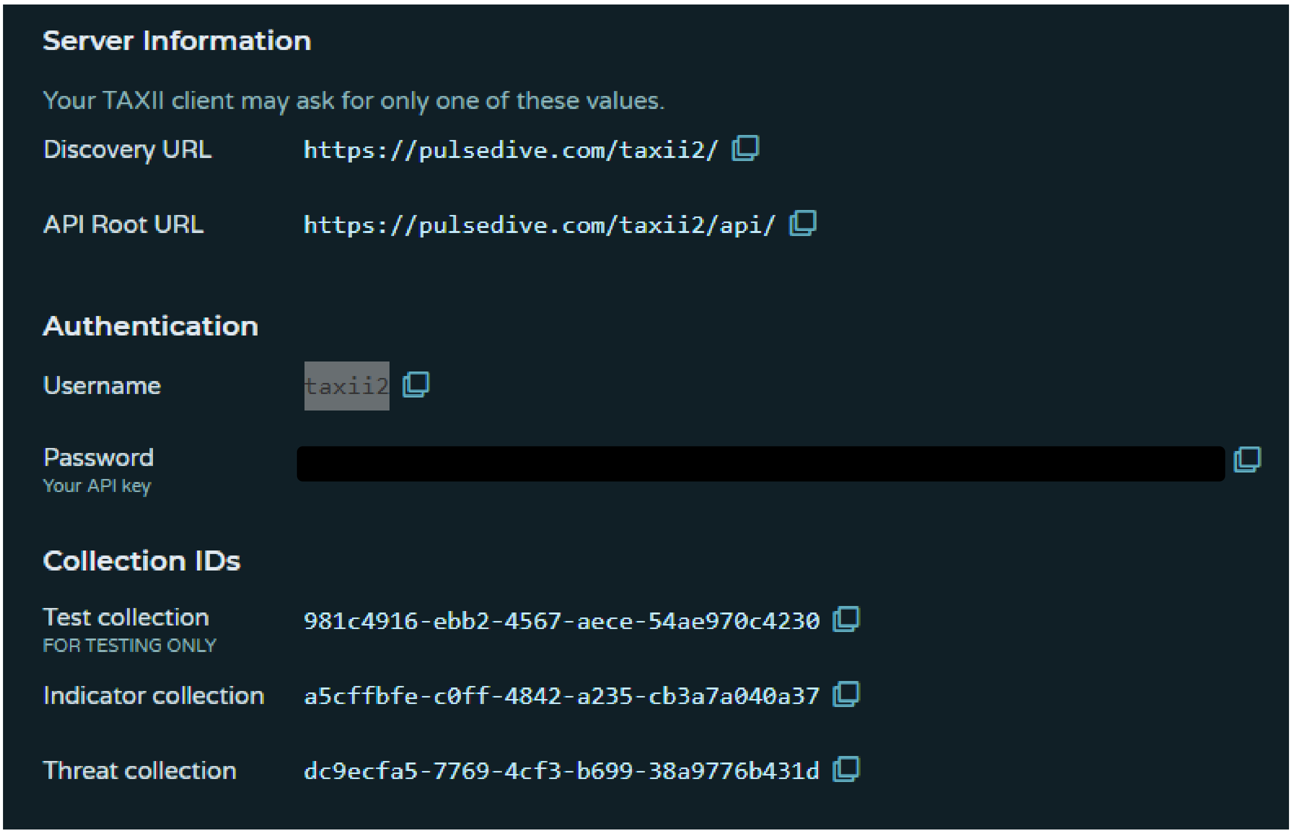
Pulsedive test data

Collection ID: 981c4916-ebb2-4567-aece-54ae970c4230

This is a test collection containing live, **sample indicator** objects.

It is available to anyone for free, for the purposes of testing, debugging, or even just learning about STIX and TAXII.

Fig 63



Server Information

Your TAXII client may ask for only one of these values.

Discovery URL	https://pulsedive.com/taxii2/
API Root URL	https://pulsedive.com/taxii2/api/

Authentication

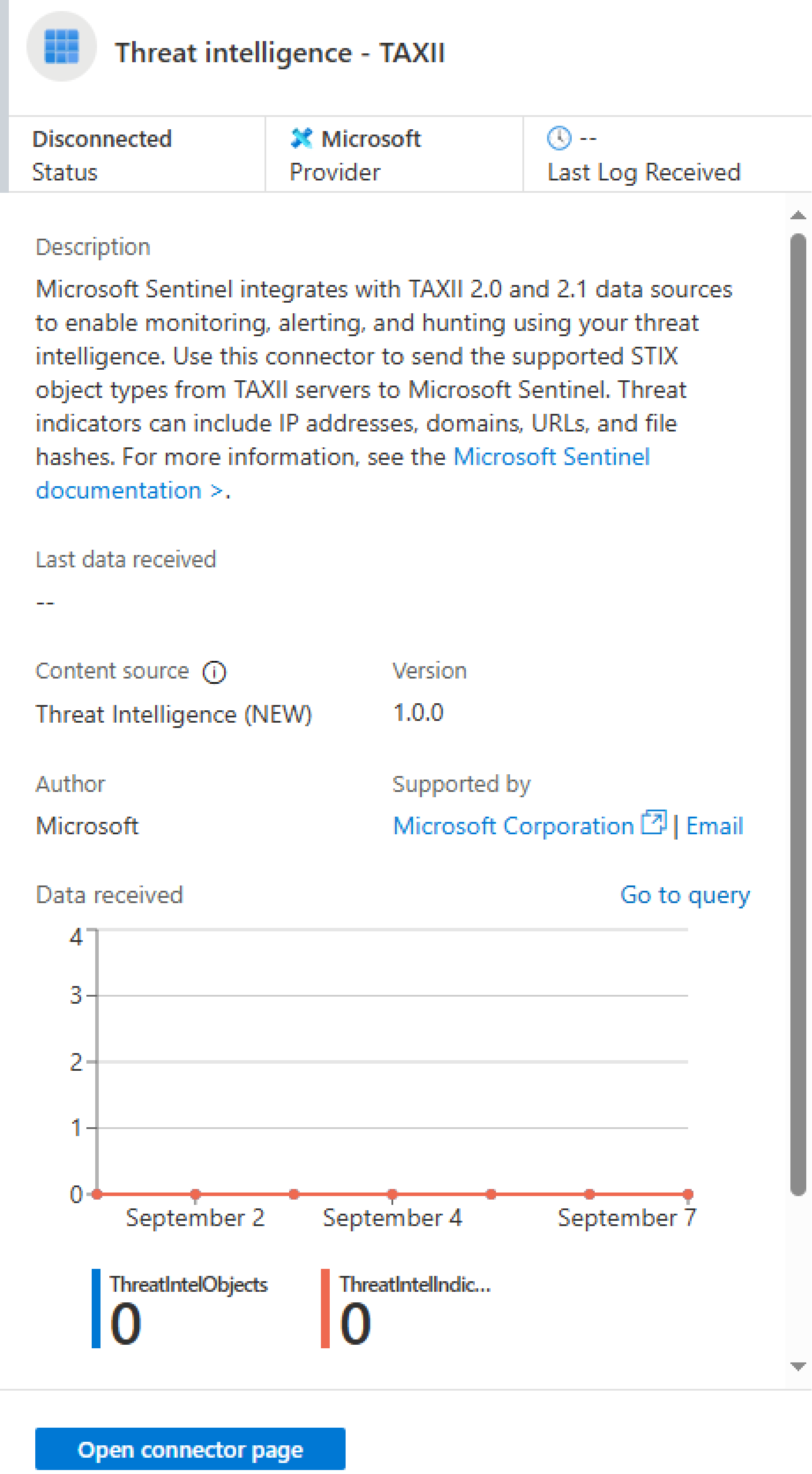
Username	taxii2
Password Your API key	[redacted]

Collection IDs

Test collection FOR TESTING ONLY	981c4916-ebb2-4567-aece-54ae970c4230
Indicator collection	a5cffbfe-c0ff-4842-a235-cb3a7a040a37
Threat collection	dc9ecfa5-7769-4cf3-b699-38a9776b431d

Fig 64

On the Threat Intelligence page, click on Open connector page



Threat intelligence - TAXII

Disconnected	Microsoft	--
Status	Provider	Last Log Received

Description

Microsoft Sentinel integrates with TAXII 2.0 and 2.1 data sources to enable monitoring, alerting, and hunting using your threat intelligence. Use this connector to send the supported STIX object types from TAXII servers to Microsoft Sentinel. Threat indicators can include IP addresses, domains, URLs, and file hashes. For more information, see the Microsoft Sentinel documentation >.

Last data received

--

Content source ⓘ

Threat Intelligence (NEW)

Version

1.0.0

Author

Microsoft

Supported by

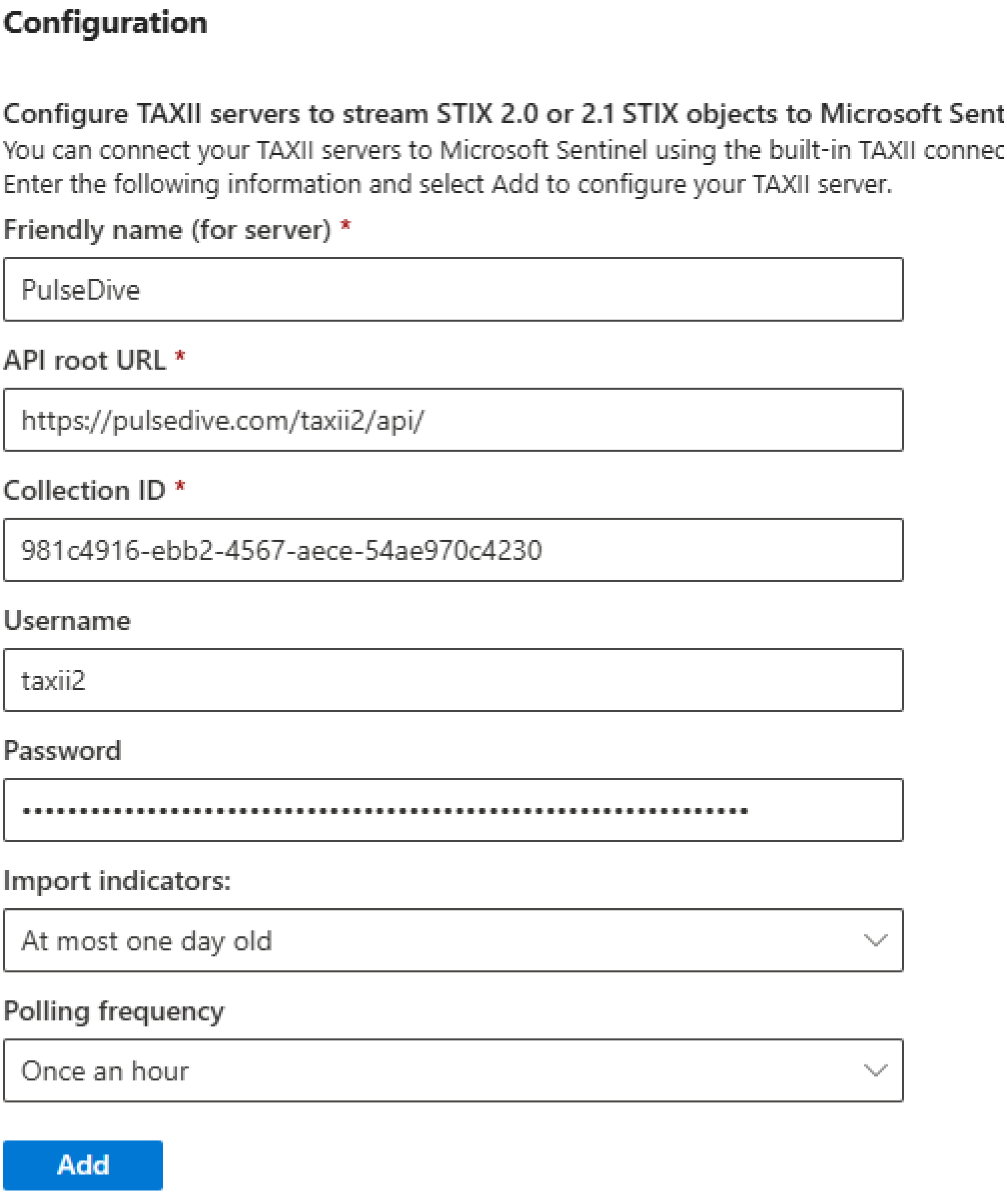
Microsoft Corporation | Email

Data received

Go to query

Fig 62

Fill in the details required as shown in fig 64 and click Add



Configuration

Configure TAXII servers to stream STIX 2.0 or 2.1 STIX objects to Microsoft Sent

You can connect your TAXII servers to Microsoft Sentinel using the built-in TAXII connec

Enter the following information and select Add to configure your TAXII server.

Friendly name (for server) *

PulseDive

API root URL *

https://pulsedive.com/taxii2/api/

Collection ID *

981c4916-ebb2-4567-aece-54ae970c4230

Username

taxii2

Password

••

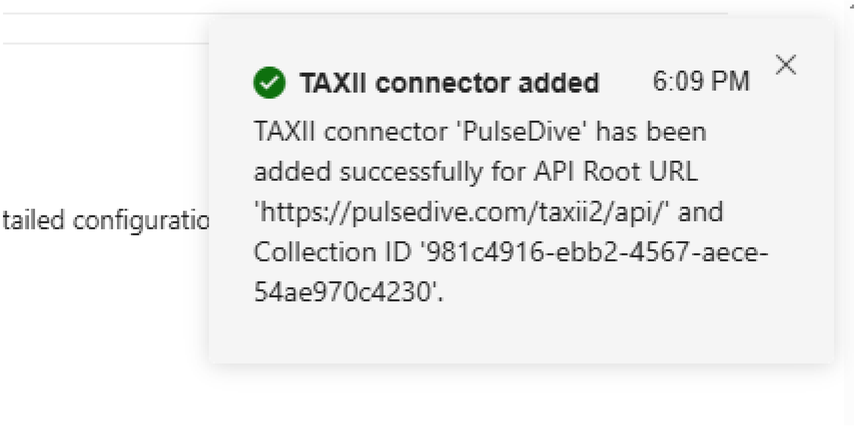
Import indicators:

At most one day old

Polling frequency

Once an hour

Fig 65

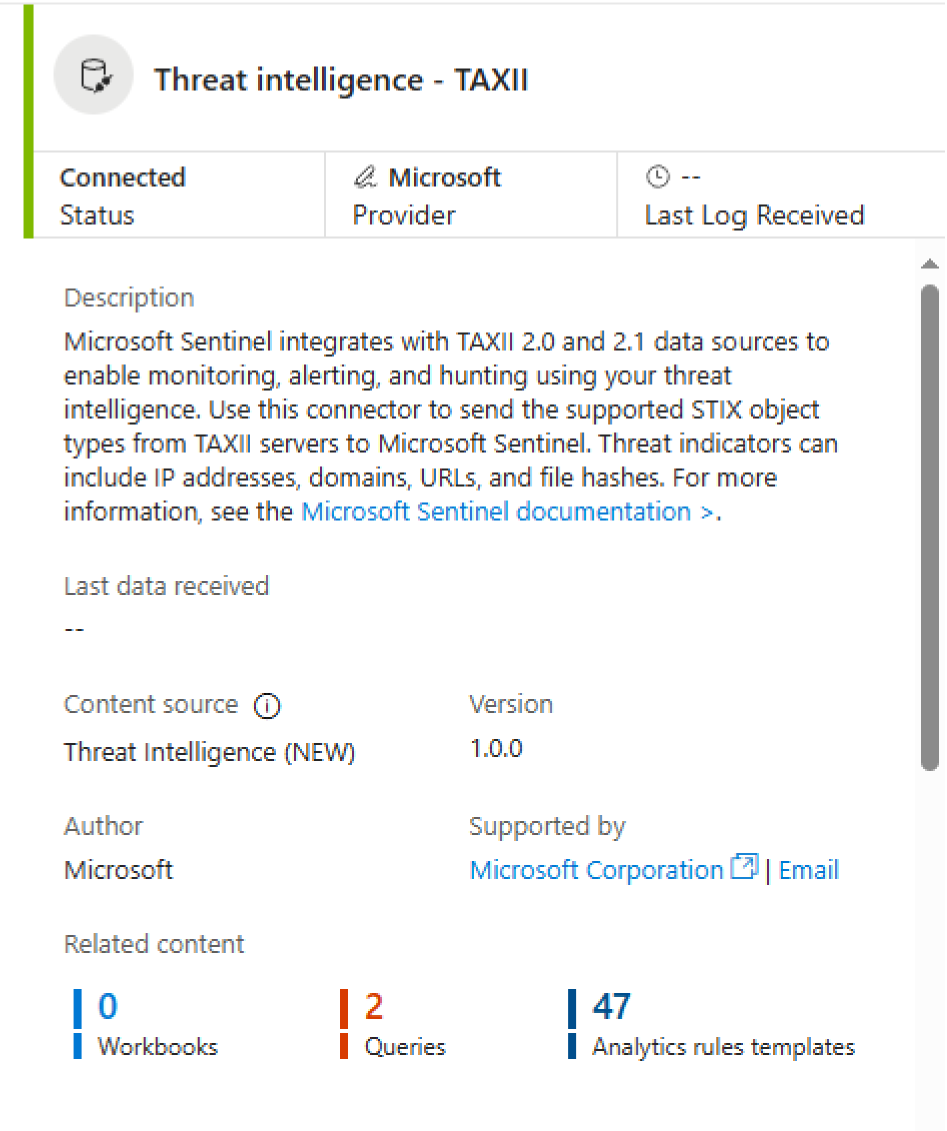


tailed configuratio

TAXII connector added 6:09 PM

TAXII connector 'PulseDive' has been added successfully for API Root URL 'https://pulsedive.com/taxii2/api/' and Collection ID '981c4916-ebb2-4567-aece-54ae970c4230'.

Fig 66



Threat intelligence - TAXII

Connected
Status

Microsoft
Provider

--
Last Log Received

Description

Microsoft Sentinel integrates with TAXII 2.0 and 2.1 data sources to enable monitoring, alerting, and hunting using your threat intelligence. Use this connector to send the supported STIX object types from TAXII servers to Microsoft Sentinel. Threat indicators can include IP addresses, domains, URLs, and file hashes. For more information, see the Microsoft Sentinel documentation >.

Last data received

--

Content source	Version
Threat Intelligence (NEW)	1.0.0

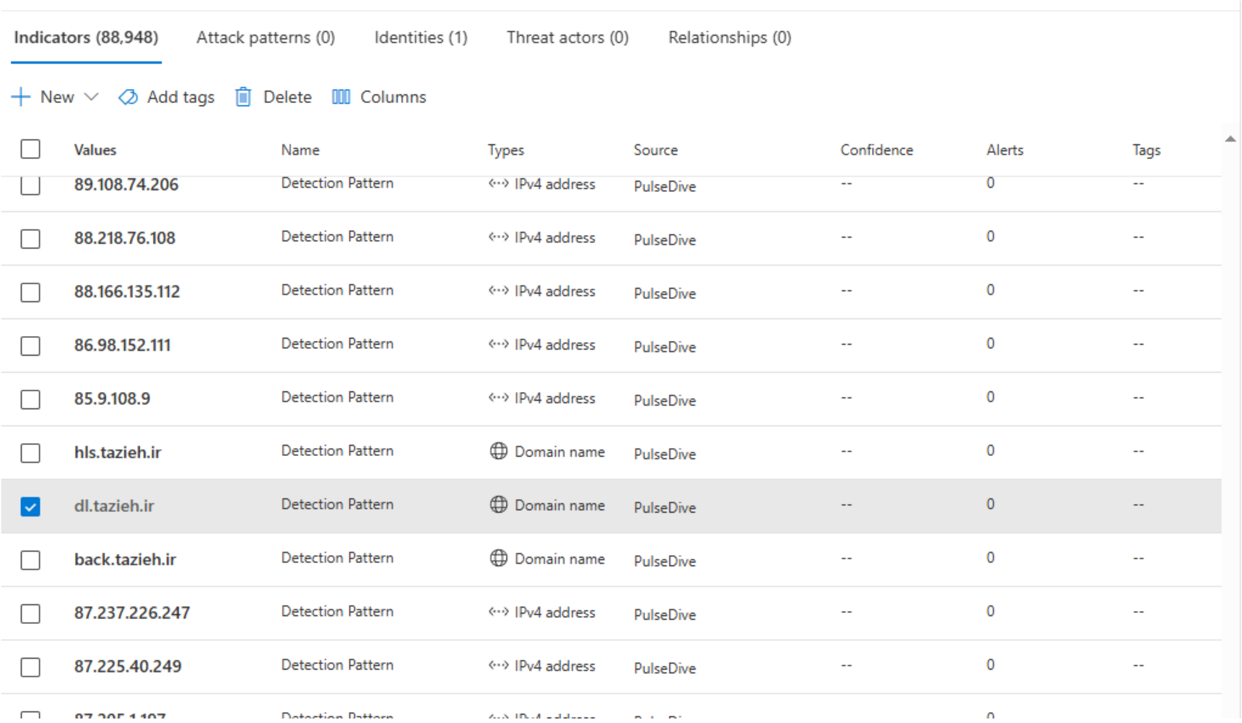
Author	Supported by
Microsoft	Microsoft Corporation | Email

Related content

0	2	47
Workbooks	Queries	Analytics rules templates

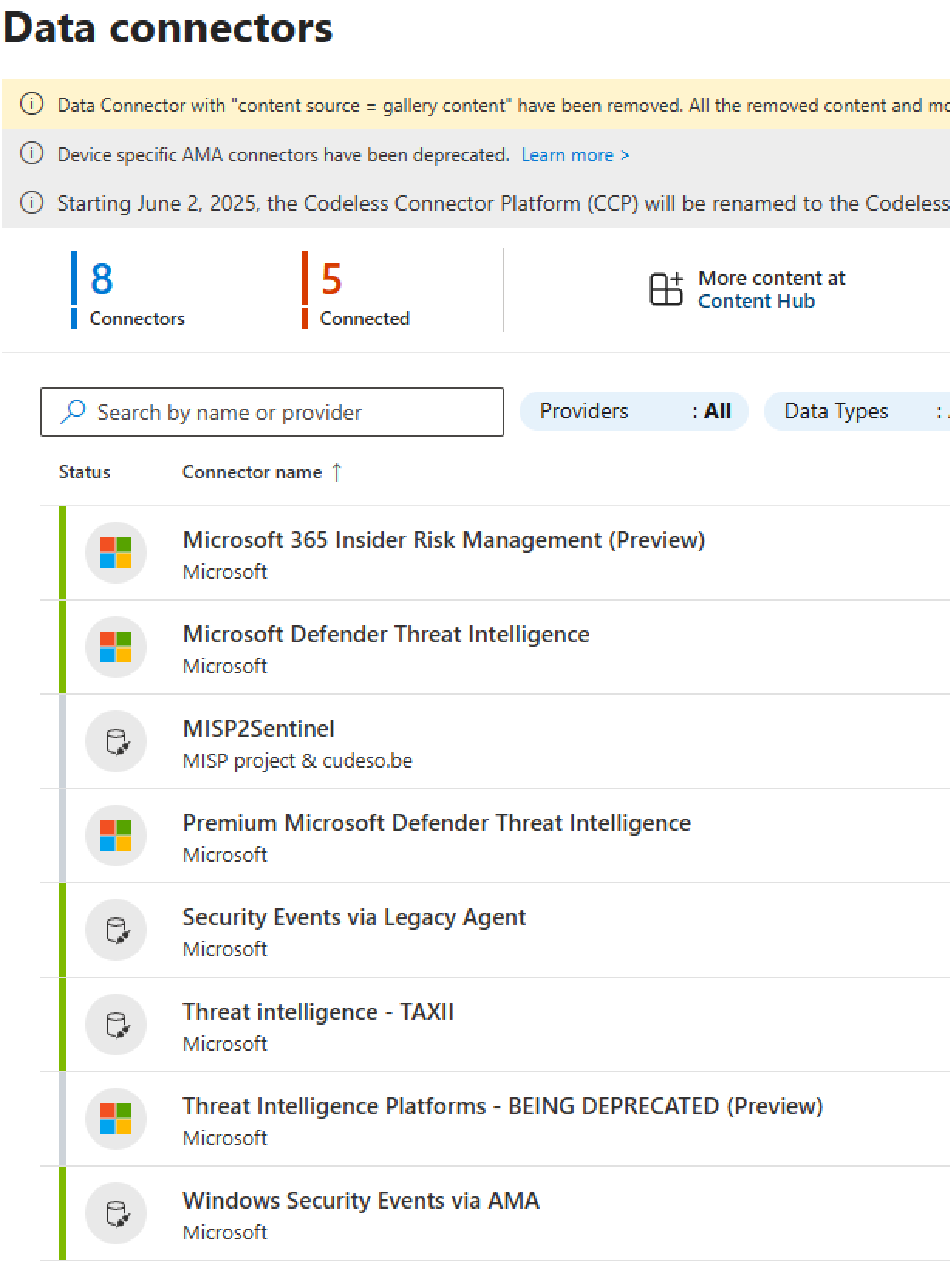
Fig 67

After a while, data from Pulsedive will be ingested into Sentinel.



☐	Values	Name	Types	Source	Confidence	Alerts	Tags
☐	89.108.74.206	Detection Pattern	IPv4 address	PulseDive	--	0	--
☐	88.218.76.108	Detection Pattern	IPv4 address	PulseDive	--	0	--
☐	88.166.135.112	Detection Pattern	IPv4 address	PulseDive	--	0	--
☐	86.98.152.111	Detection Pattern	IPv4 address	PulseDive	--	0	--
☐	85.9.108.9	Detection Pattern	IPv4 address	PulseDive	--	0	--
☐	hls.tazieh.ir	Detection Pattern	Domain name	PulseDive	--	0	--
☑	dl.tazieh.ir	Detection Pattern	Domain name	PulseDive	--	0	--
☐	back.tazieh.ir	Detection Pattern	Domain name	PulseDive	--	0	--
☐	87.237.226.247	Detection Pattern	IPv4 address	PulseDive	--	0	--
☐	87.225.40.249	Detection Pattern	IPv4 address	PulseDive	--	0	--
☐	87.205.1.107	Detection Pattern	IPv4 address	PulseDive		0	

Fig 68



Data connectors

ⓘ Data Connector with "content source = gallery content" have been removed. All the removed content and mo

ⓘ Device specific AMA connectors have been deprecated. Learn more >

ⓘ Starting June 2, 2025, the Codeless Connector Platform (CCP) will be renamed to the Codeless

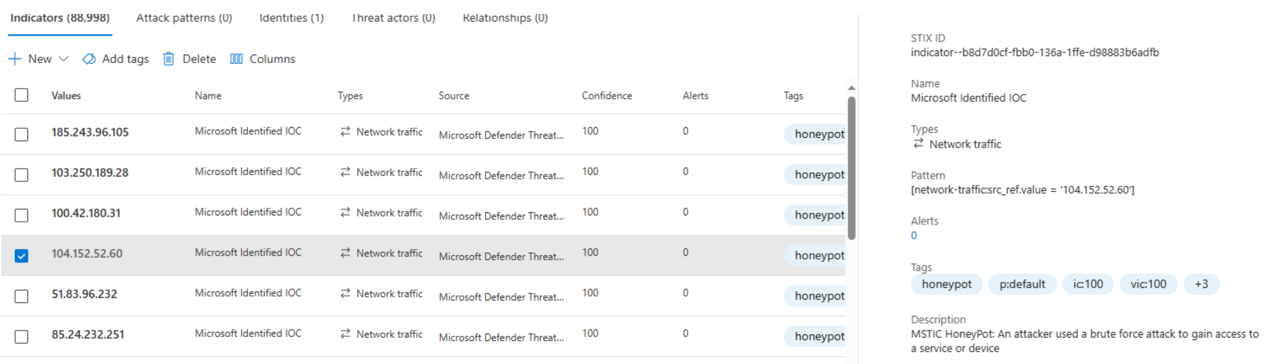
8 Connectors

5 Connected

More content at Content Hub

Status	Connector name ↑
🟩	Microsoft 365 Insider Risk Management (Preview) Microsoft
🟩	Microsoft Defender Threat Intelligence Microsoft
⬜	MISP2Sentinel MISP project & cudeso.be
⬜	Premium Microsoft Defender Threat Intelligence Microsoft
🟩	Security Events via Legacy Agent Microsoft
🟩	Threat intelligence - TAXII Microsoft
⬜	Threat Intelligence Platforms - BEING DEPRECATED (Preview) Microsoft
🟩	Windows Security Events via AMA Microsoft

Fig 69



□	Values	Name	Types	Source	Confidence	Alerts	Tags
□	185.243.96.105	Microsoft Identified IOC	⇄ Network traffic	Microsoft Defender Threat...	100	0	honeypot
□	103.250.189.28	Microsoft Identified IOC	⇄ Network traffic	Microsoft Defender Threat...	100	0	honeypot
□	100.42.180.31	Microsoft Identified IOC	⇄ Network traffic	Microsoft Defender Threat...	100	0	honeypot
☑	104.152.52.60	Microsoft Identified IOC	⇄ Network traffic	Microsoft Defender Threat...	100	0	honeypot
□	51.83.96.232	Microsoft Identified IOC	⇄ Network traffic	Microsoft Defender Threat...	100	0	honeypot
□	85.24.232.251	Microsoft Identified IOC	⇄ Network traffic	Microsoft Defender Threat...	100	0	honeypot

STIX ID
indicator--b8d7d0cf-fbb0-136a-1ffe-d98883b6adfb

Name
Microsoft Identified IOC

Types
⇄ Network traffic

Pattern
[network-traffic:src_ref.value = '104.152.52.60']

Alerts
0

Tags
honeypot p:default ic:100 vic:100 +3

Description
MSTIC HoneyPot: An attacker used a brute force attack to gain access to a service or device

Fig 70

Conclusion:

The SOC simulation successfully demonstrated the process of detecting and responding to a brute force attack within a cloud-hosted environment. By deploying a Honeynet in Azure and integrating security telemetry into Microsoft Sentinel, the exercise highlighted the effectiveness of centralized log collection, monitoring, and incident management. The manual creation and assignment of an incident ticket reinforced the critical role of SOC analysts in the investigation workflow.

Additionally, configuring Pulsedive as a threat intelligence data connector provided valuable enrichment capabilities. This integration enhanced the detection process by correlating observed indicators with external threat intelligence, thereby improving the accuracy and context of incident analysis.

Overall, the simulation illustrated how cloud-native SOC tools and threat intelligence can be combined to strengthen proactive defense and incident response capabilities.

Key Learnings & Recommendations

Key Learnings

1. **Value of Centralized Monitoring:** Forwarding logs from the Honeynet to Microsoft Sentinel provided a unified view of system activity, demonstrating the importance of centralized monitoring for rapid threat detection.
2. **Detection of Real-World Threats:** The successful identification of a brute force attack emphasized Sentinel's capability to detect common adversarial techniques when properly configured.
3. **Role of Threat Intelligence:** Integrating Pulsedive enriched the investigation process by mapping observed indicators of compromise (IOCs) against external threat feeds, adding context and confidence to detections.
4. **Incident Handling Workflow:** The manual creation and assignment of incidents reinforced the structured workflow SOC analysts follow, from detection to investigation and resolution.
5. **Cloud-Native Security Advantage:** Leveraging Azure services showcased the flexibility and scalability of cloud-based SOC operations compared to traditional on-premises setups.

Recommendations

- **Automate Incident Response:** Implement automation playbooks in Sentinel (via Logic Apps) to reduce manual effort in ticket creation and response.
- **Expand Threat Intelligence Sources:** In addition to Pulsedive, connect other threat intelligence feeds (such as MISP or ThreatConnect) to further strengthen IOC enrichment.
- **Enable Continuous Hunting:** Establish scheduled queries to automatically detect repeated attack patterns rather than relying solely on manual hunting.
- **Broaden Honeynet Scope:** Consider deploying additional VM types or operating systems to simulate a more diverse attack surface and capture a wider range of threats.

- **Refine Alert Tuning:** Adjust analytics rules to reduce false positives while ensuring that genuine threats are escalated effectively.