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

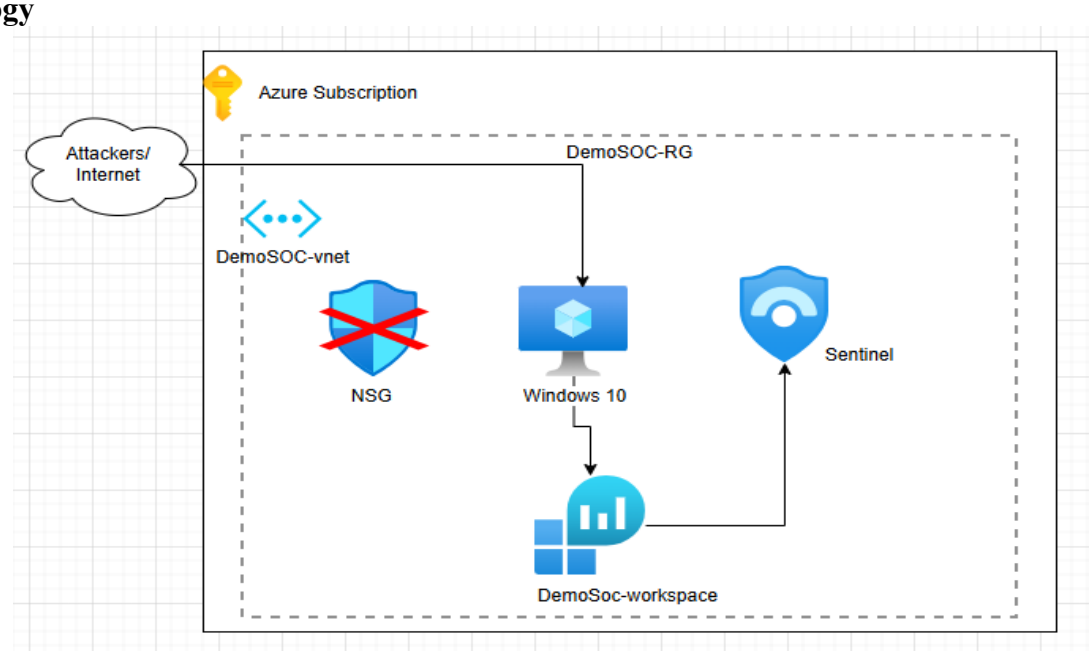

Fig 1

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.

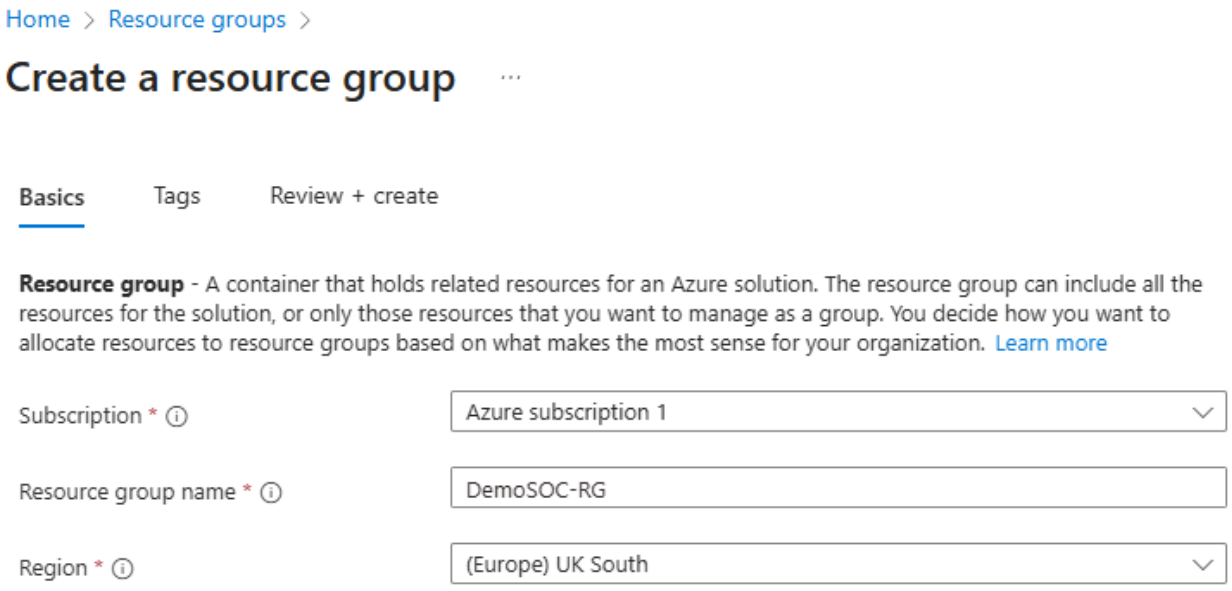

Fig 2

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

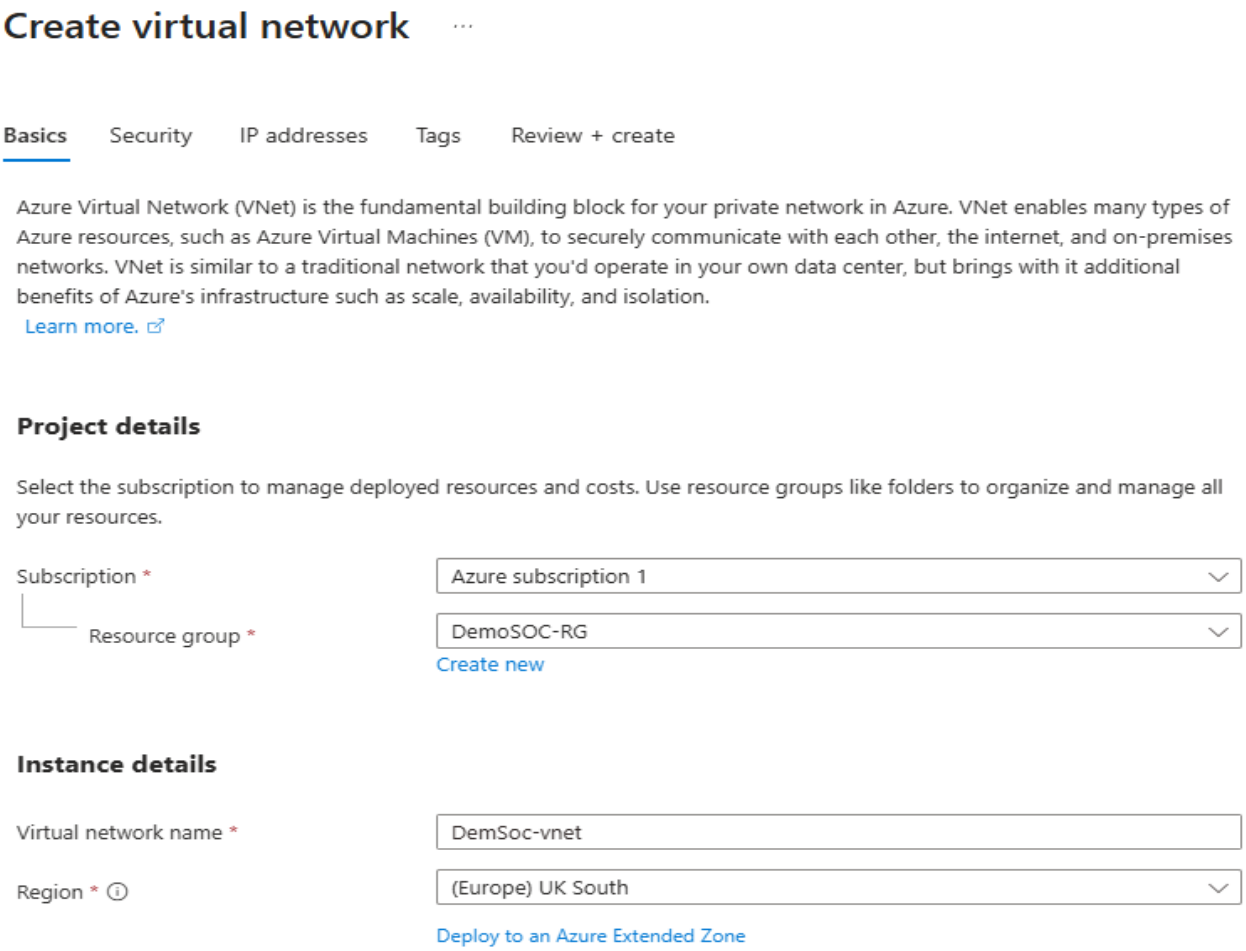

Fig 3

Create a Virtual Machine (VM)

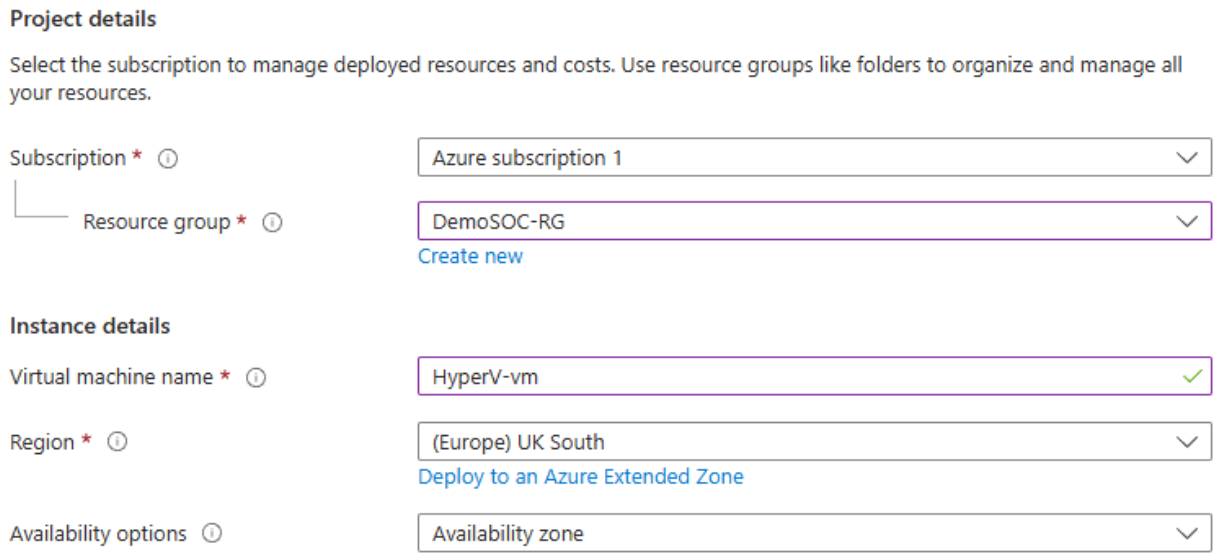

Fig 4

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

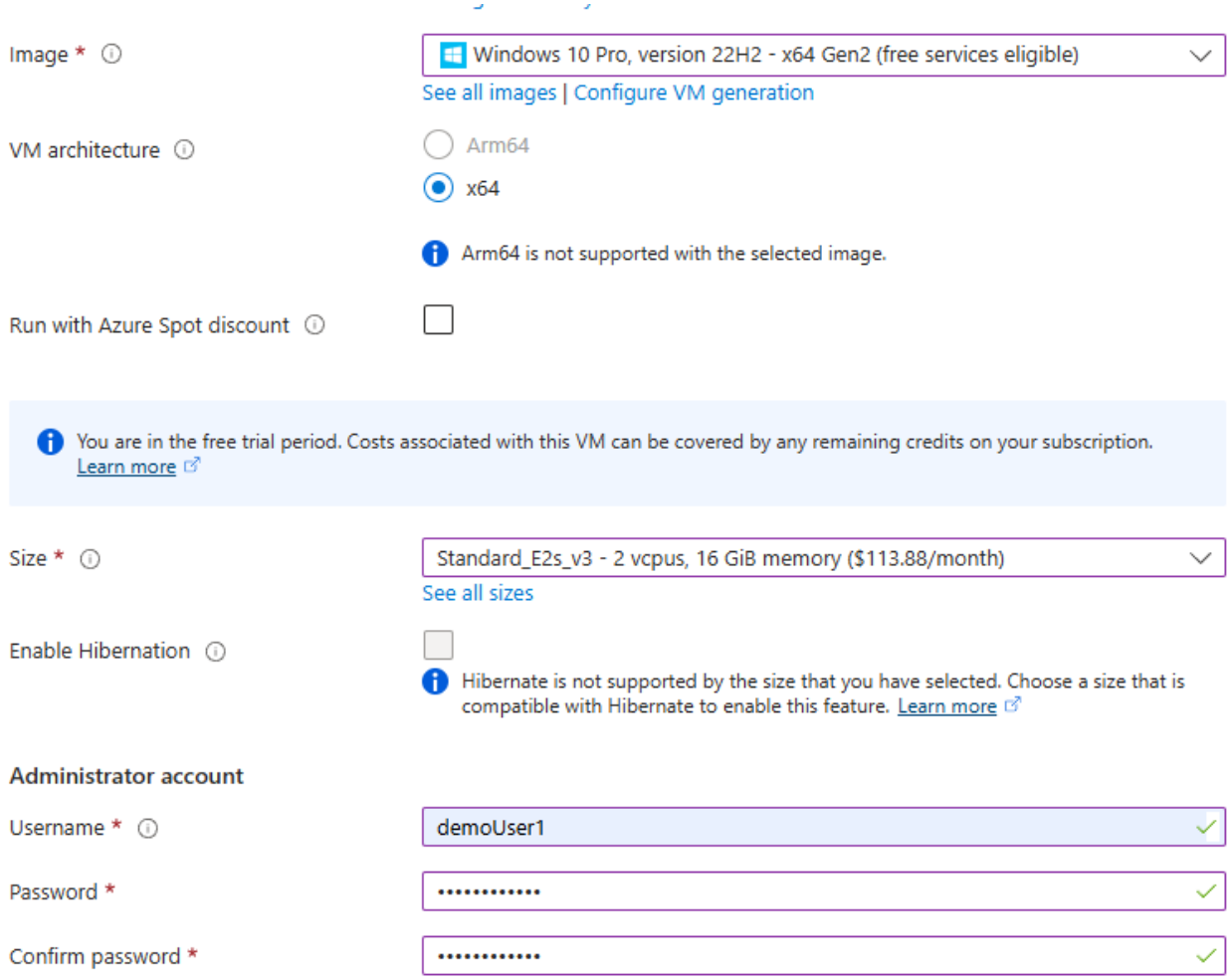

Fig 5

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.

Fig 6

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

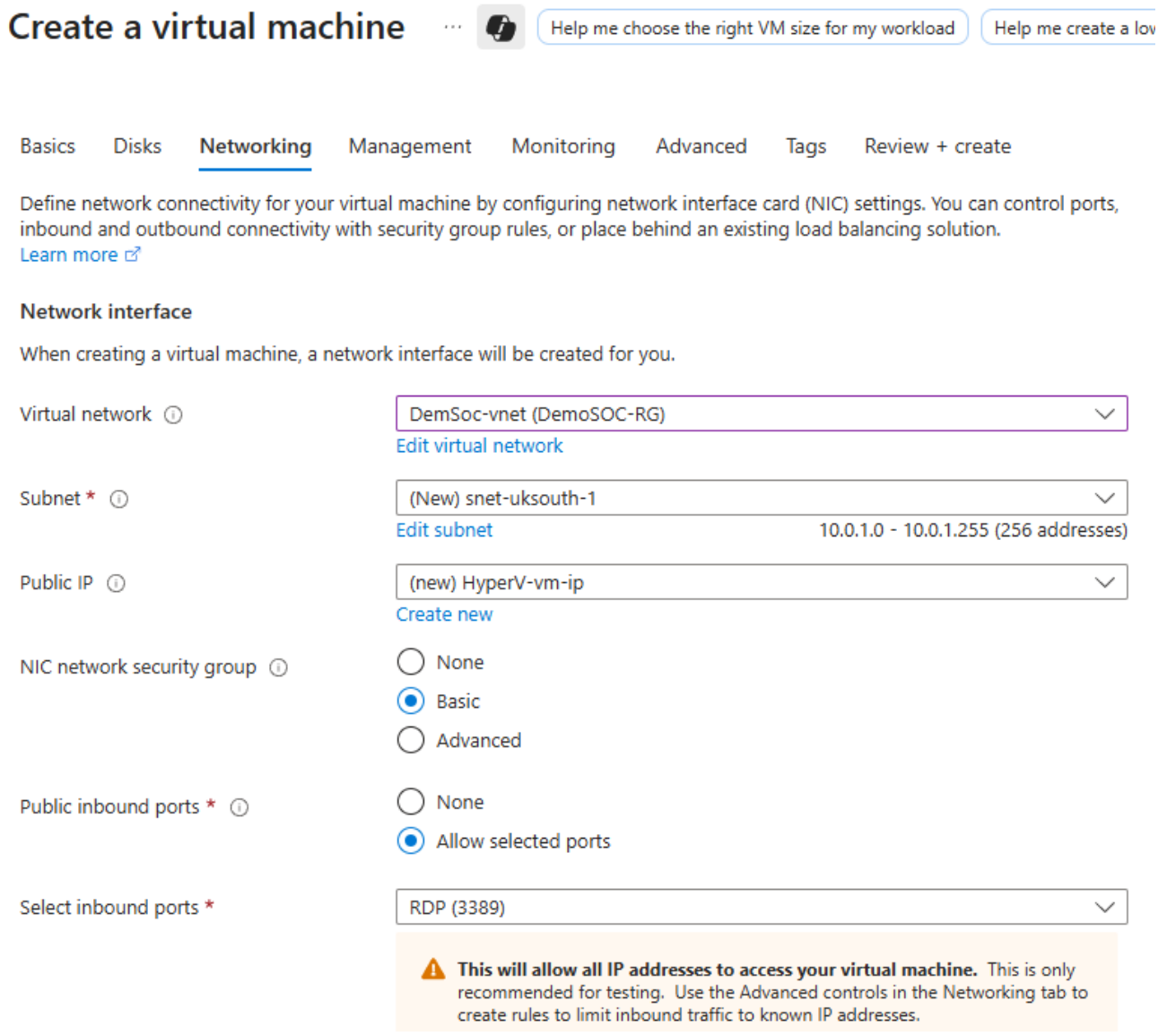

Fig 6

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

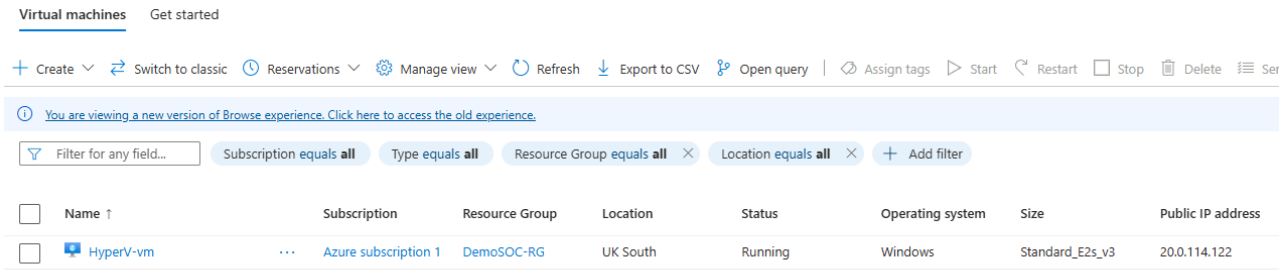

Fig 7

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

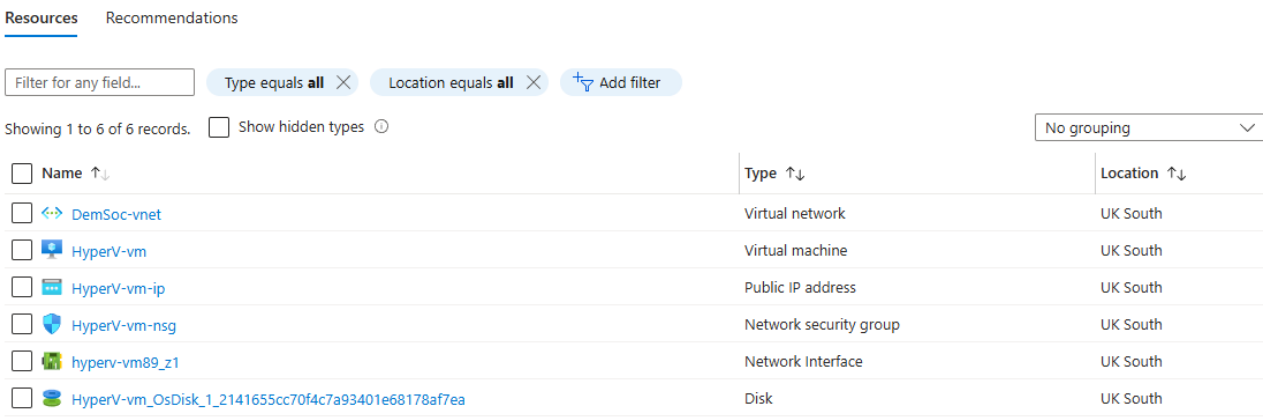

Fig 8

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.

Fig 9

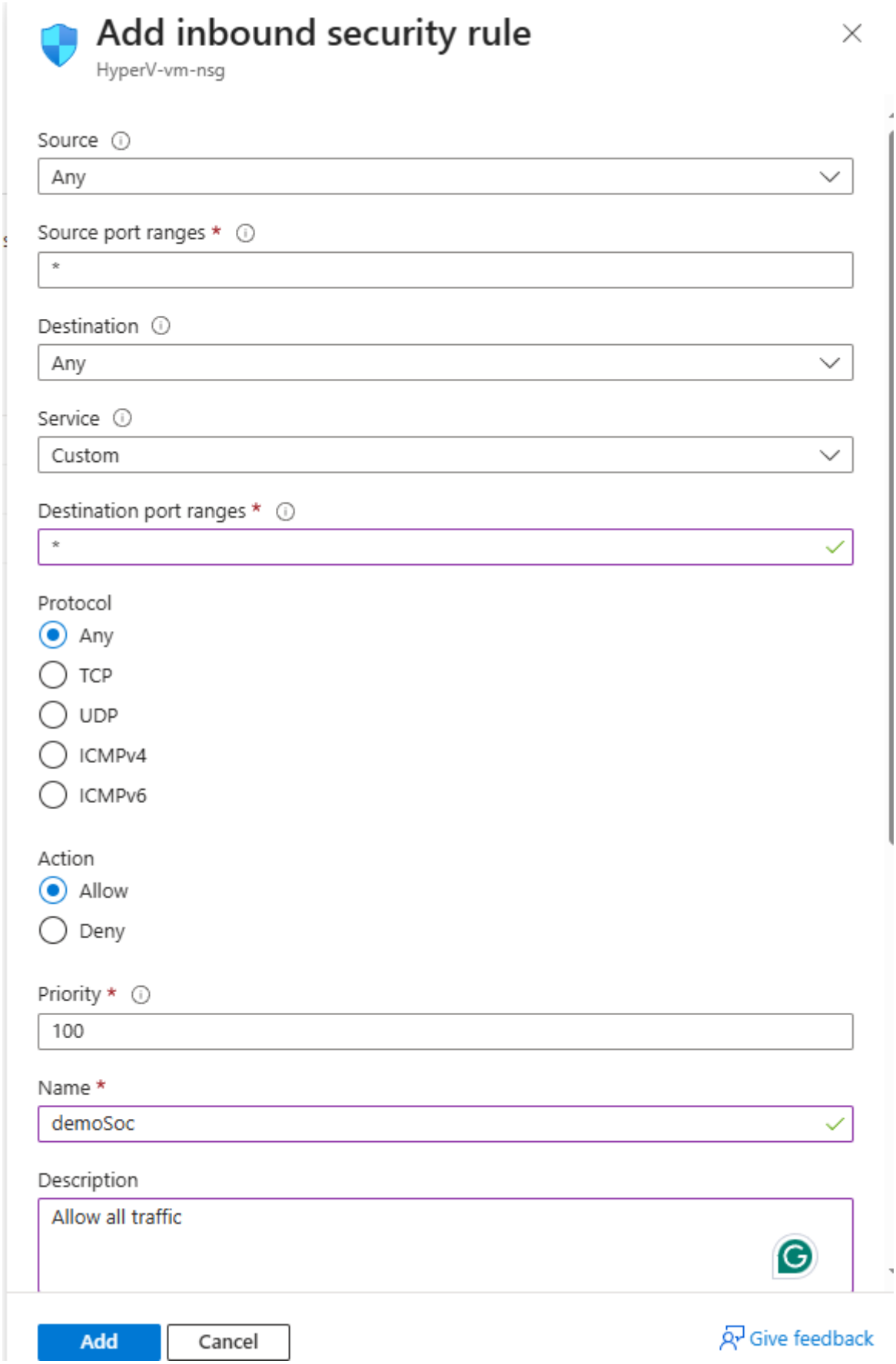
Add inbound security rule
HyperV-vm-nsg
Source
Any
Source port ranges *
*
Destination
Any
Service
Custom
Destination port ranges *
*
Protocol
Any
TCP
UDP
ICMPv4
ICMPv6
Action
Allow
Deny
Priority *
100
Name *
demoSoc
Description
Allow all traffic
Add
Cancel
Give feedback

Fig 10

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

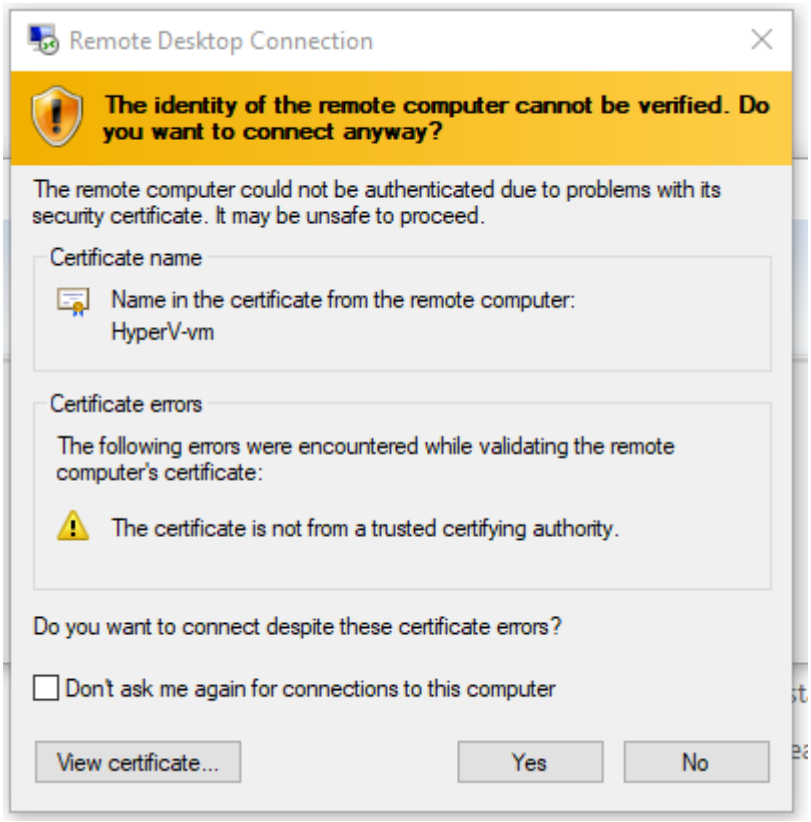

Fig 11

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

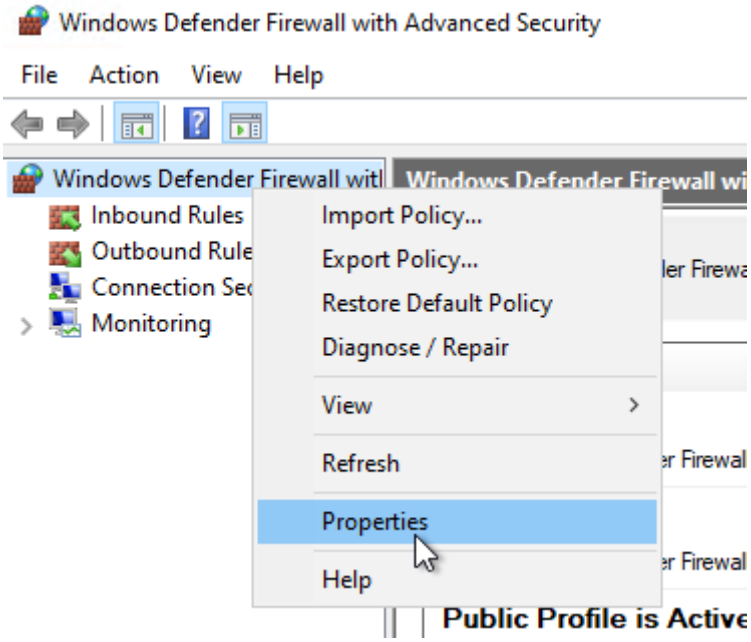

Fig 12

Disable the firewall state in all the tabs.

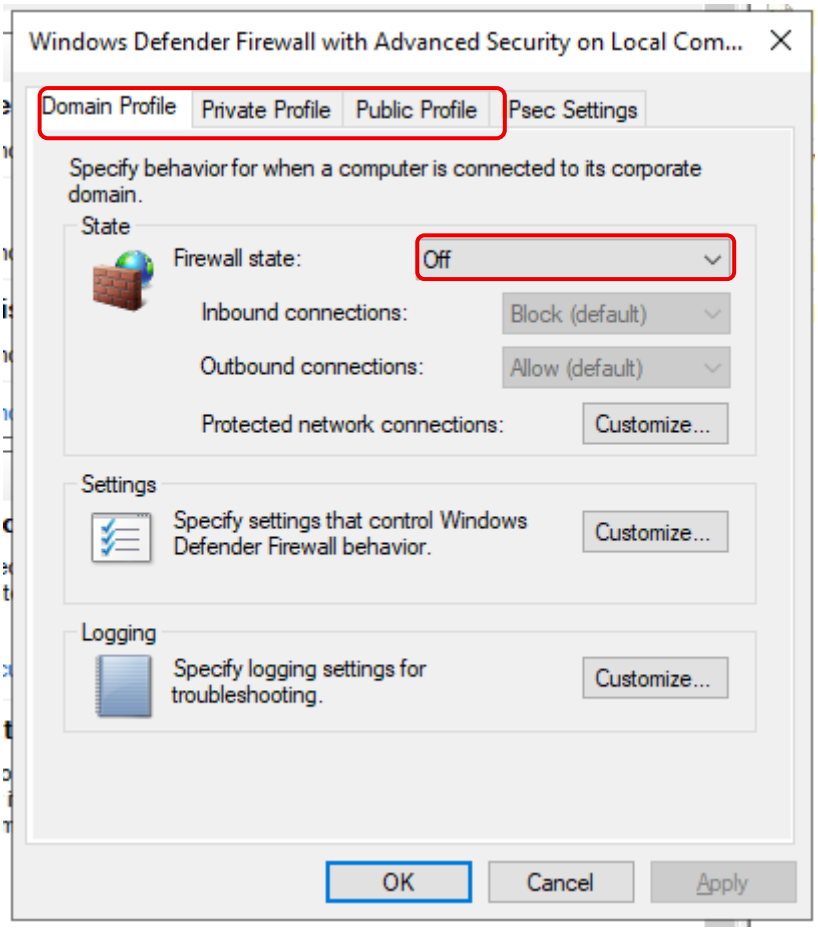

Fig 13

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.

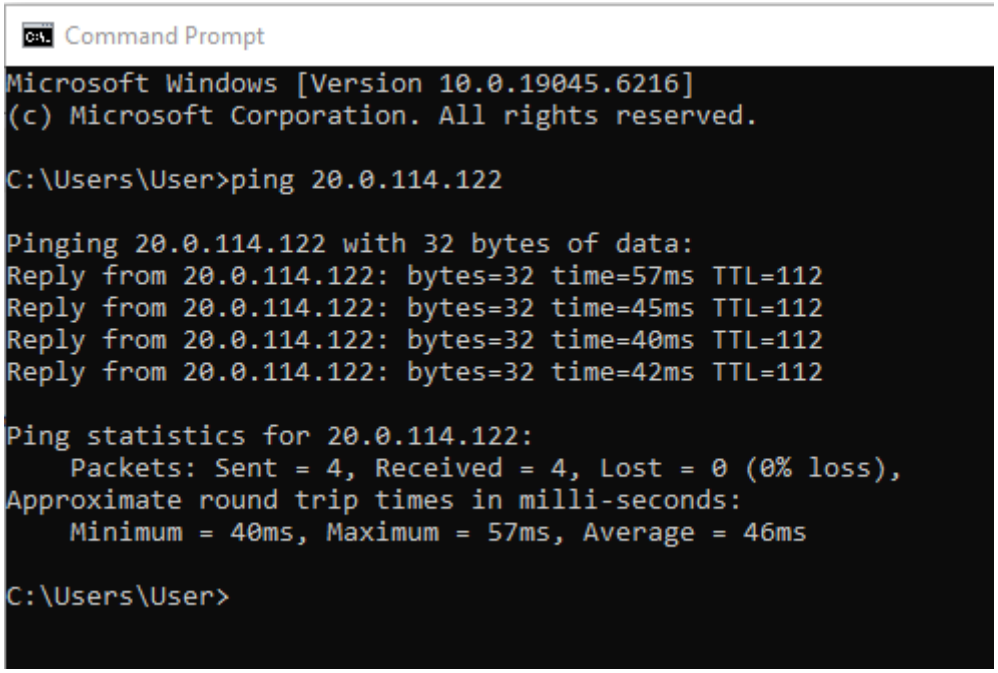

Fig 14

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

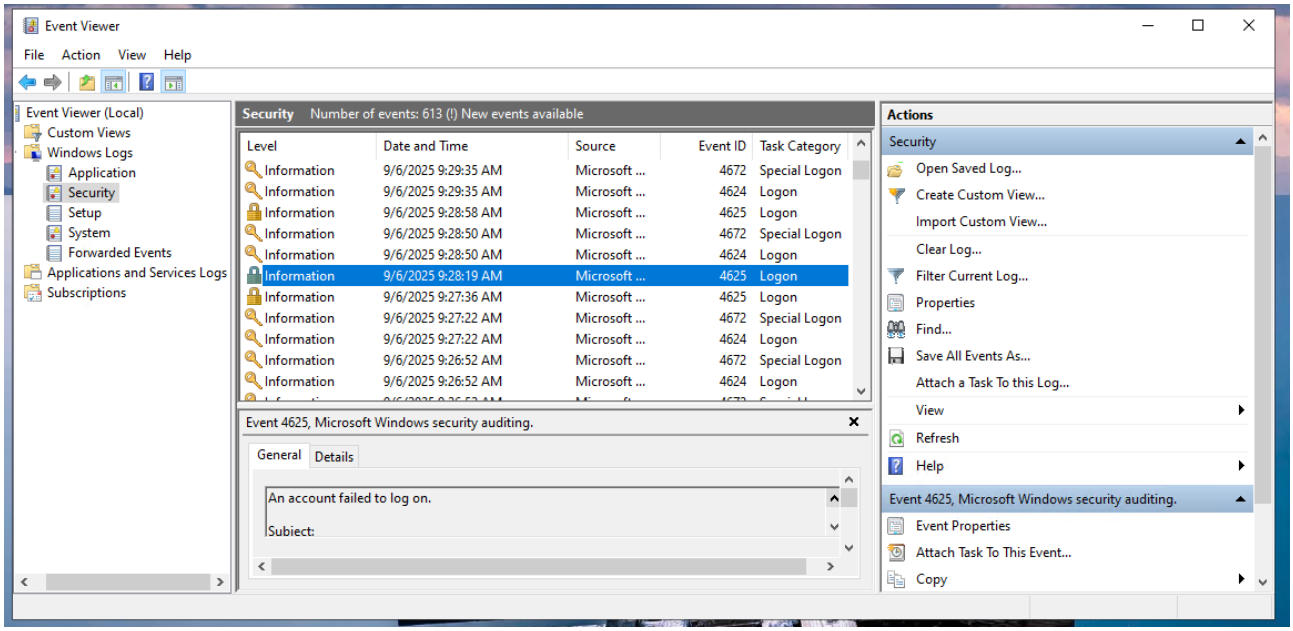

Fig 15

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

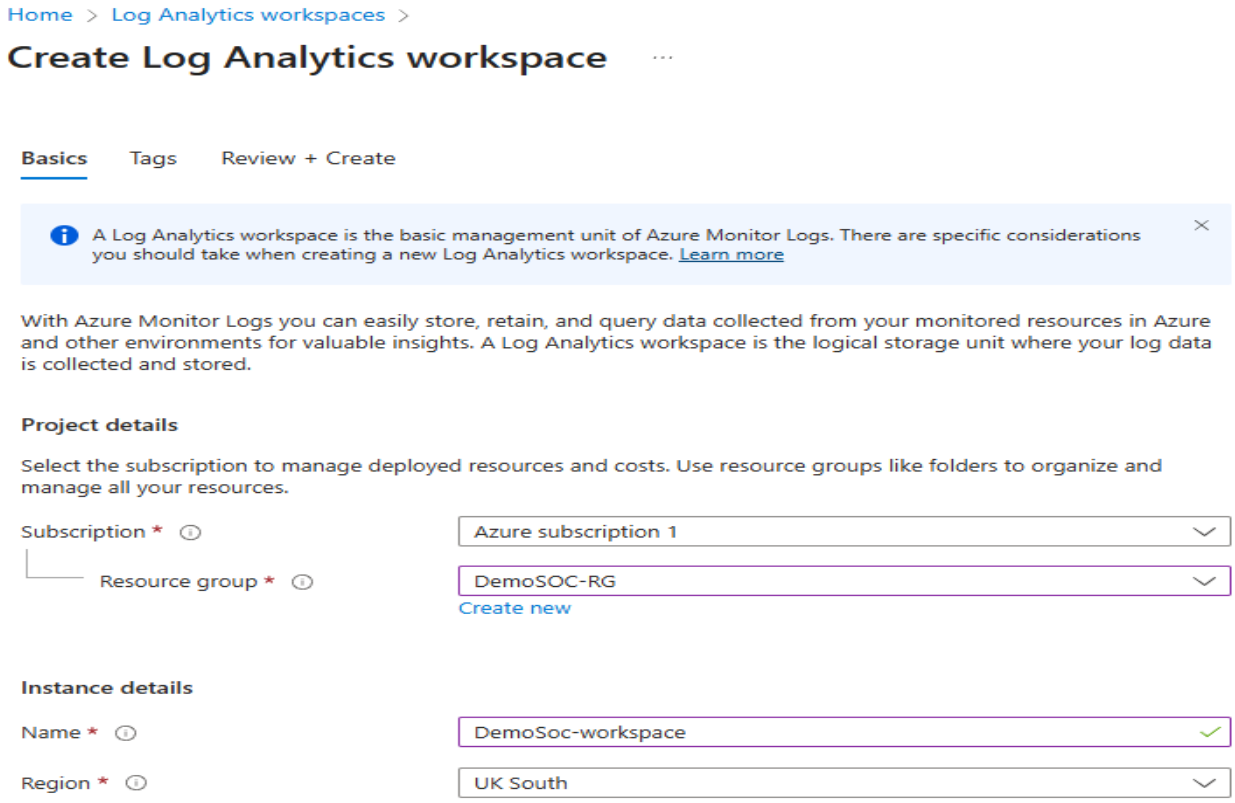

Fig 16

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

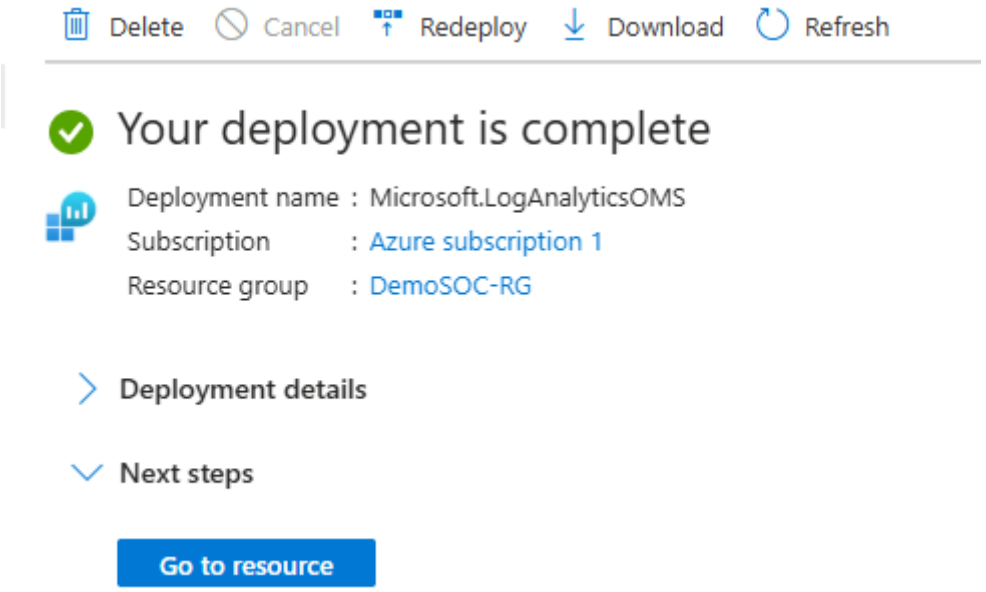

Fig 17

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

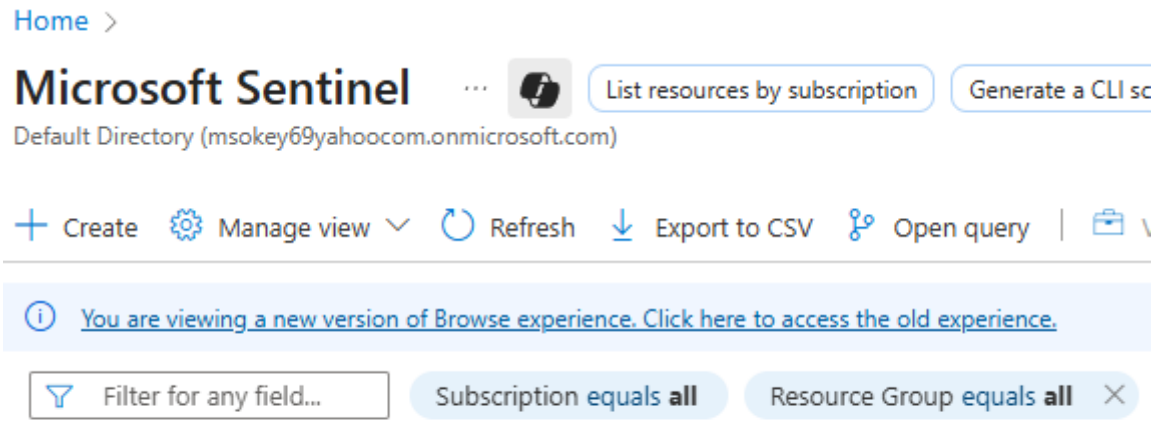

Fig 18

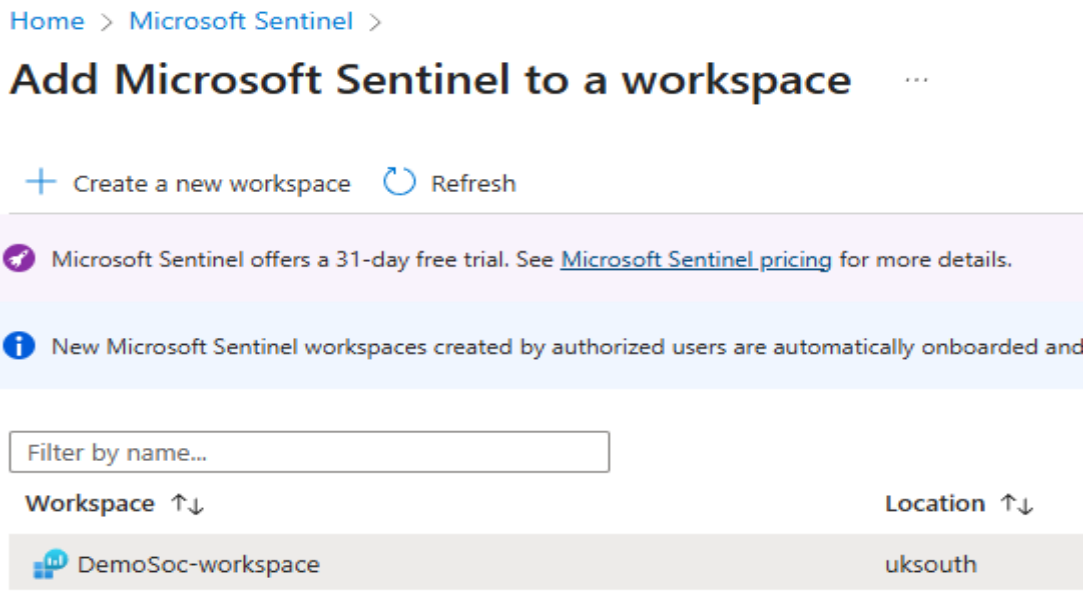

Fig 19

Select the workspace created shown above

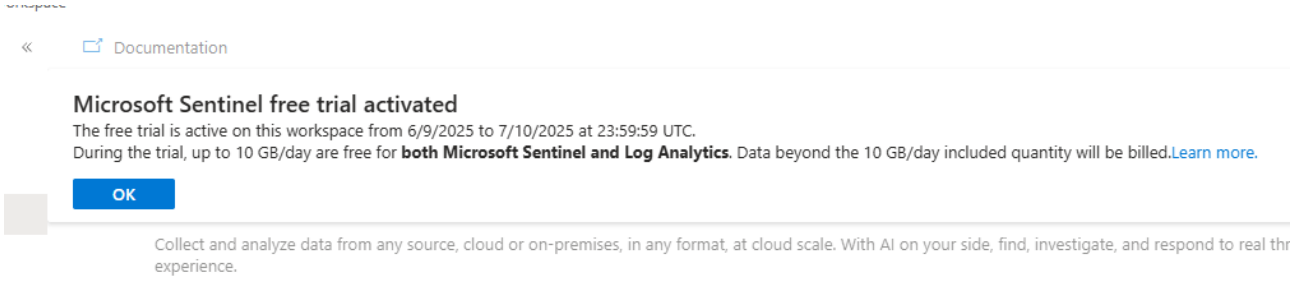

Fig 20

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

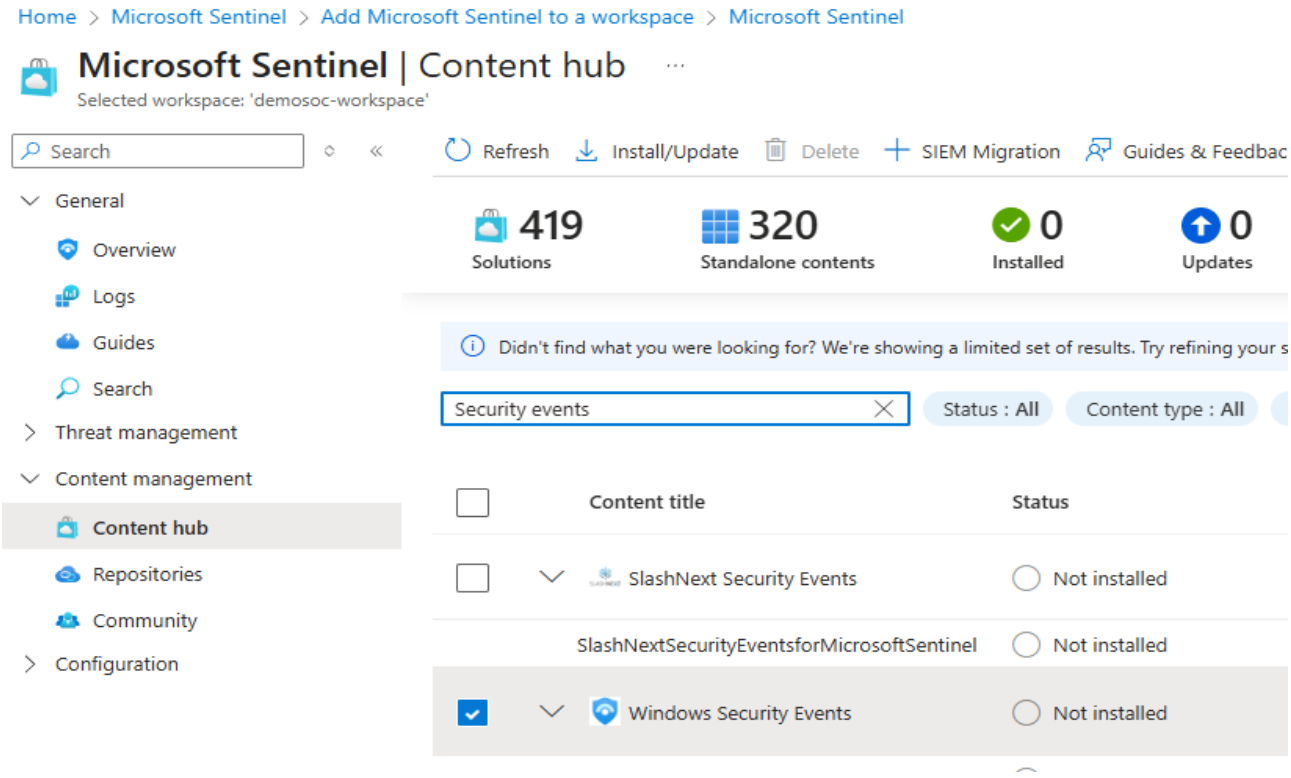

Fig 21

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

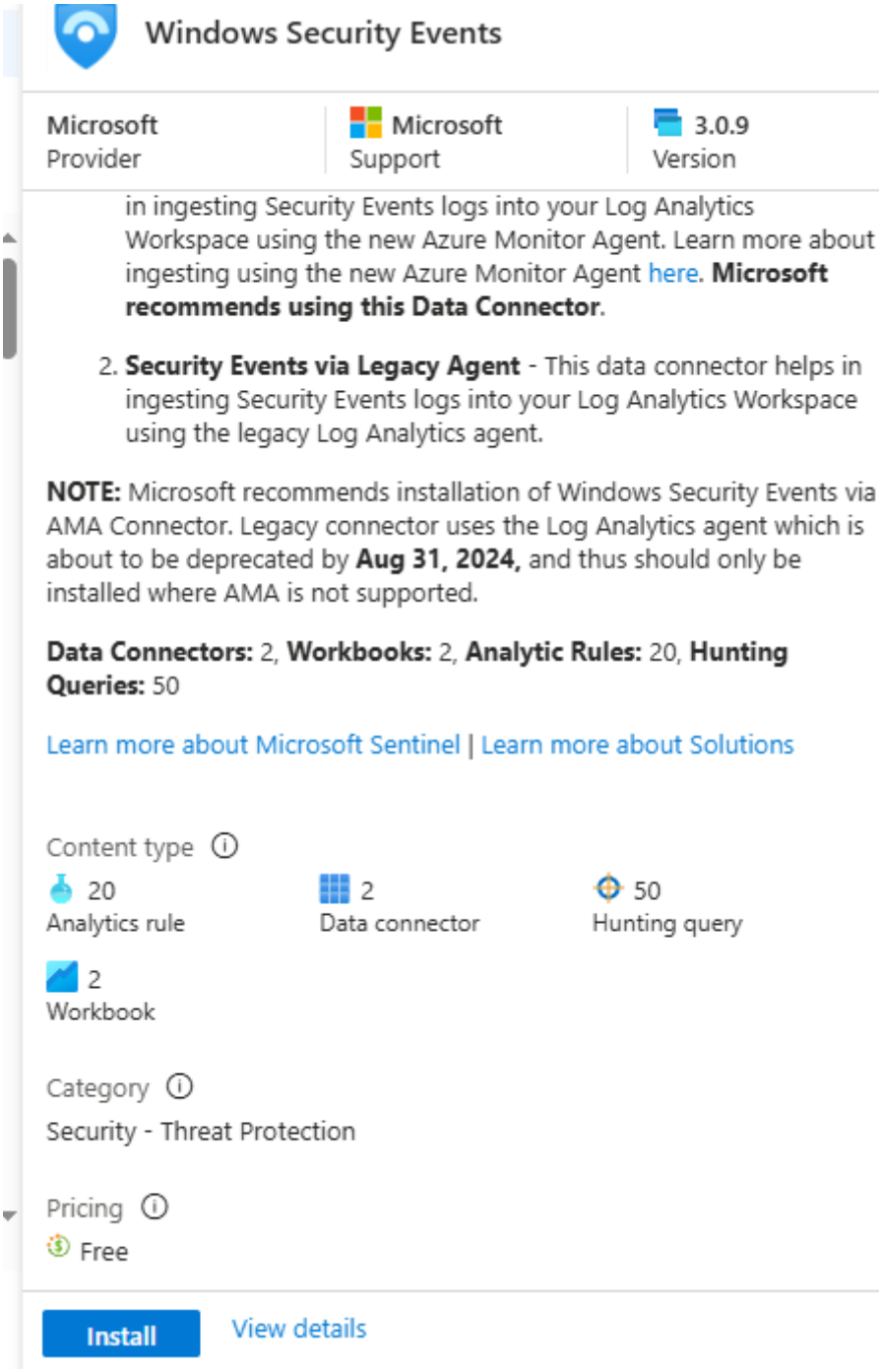

Fig 22

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

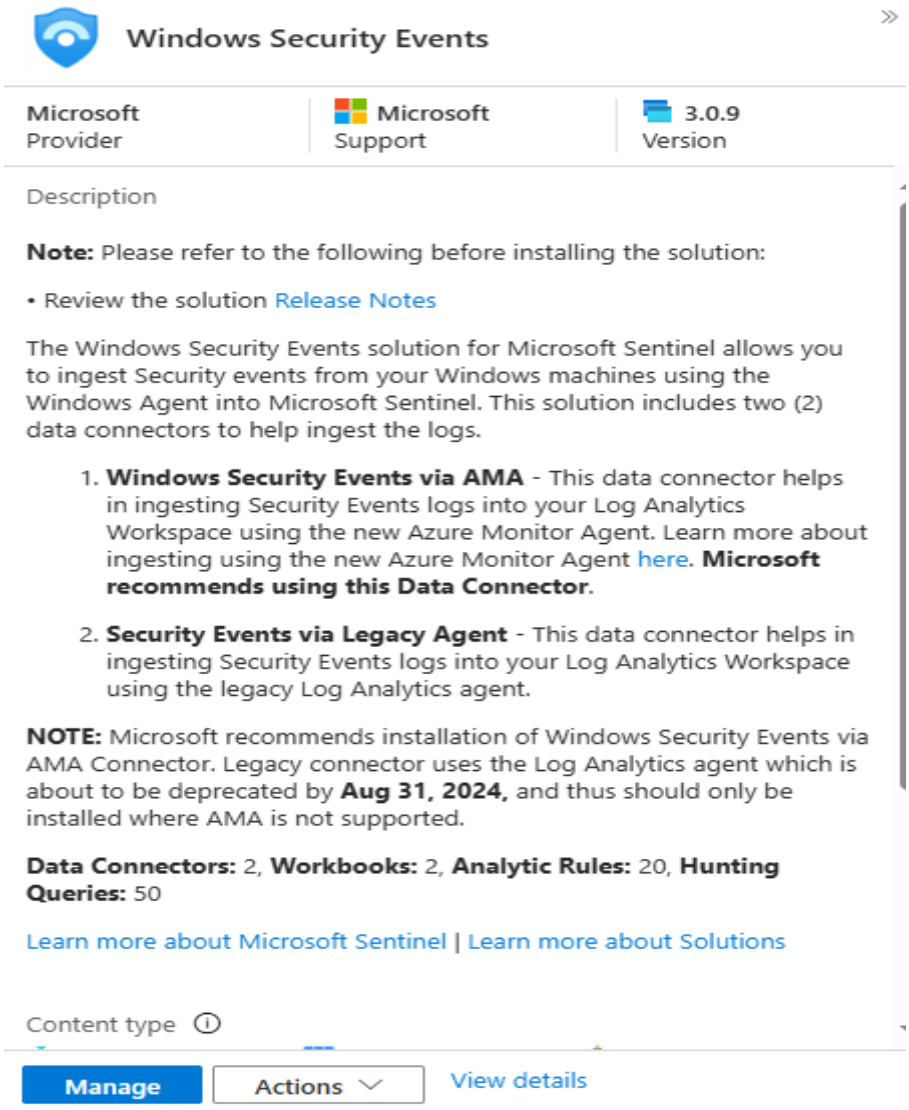

Fig 24

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

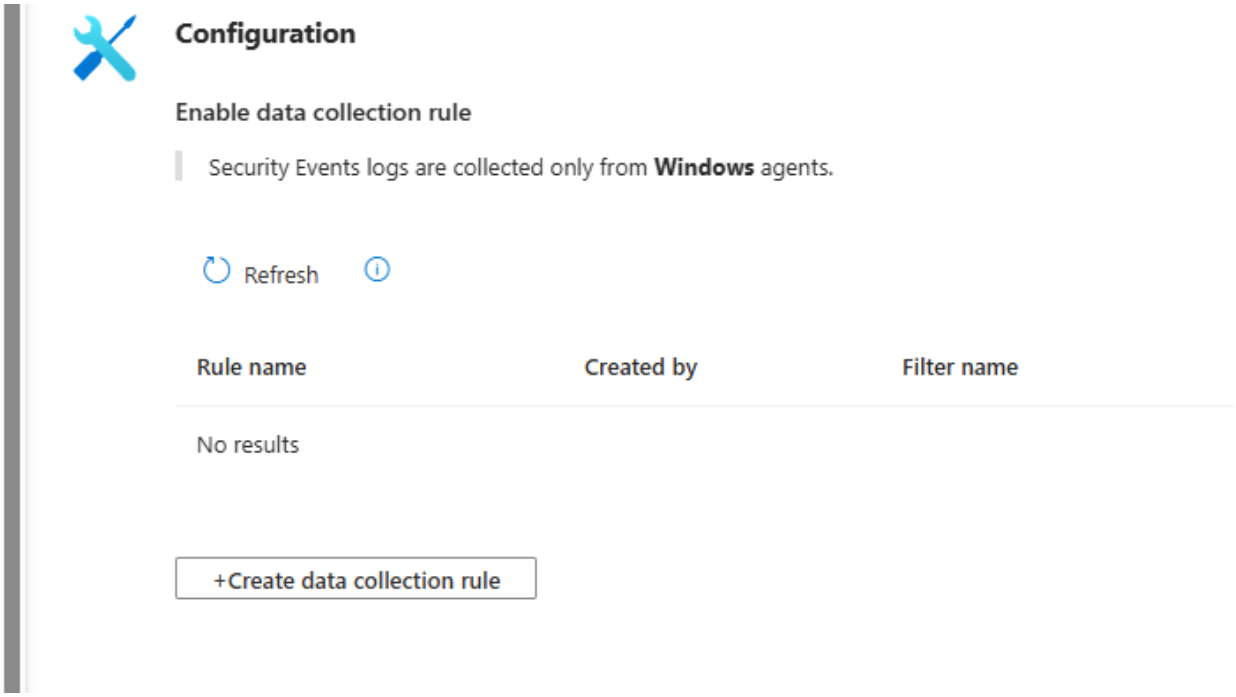

Fig 26

Give the collection rule a name. select the resource group

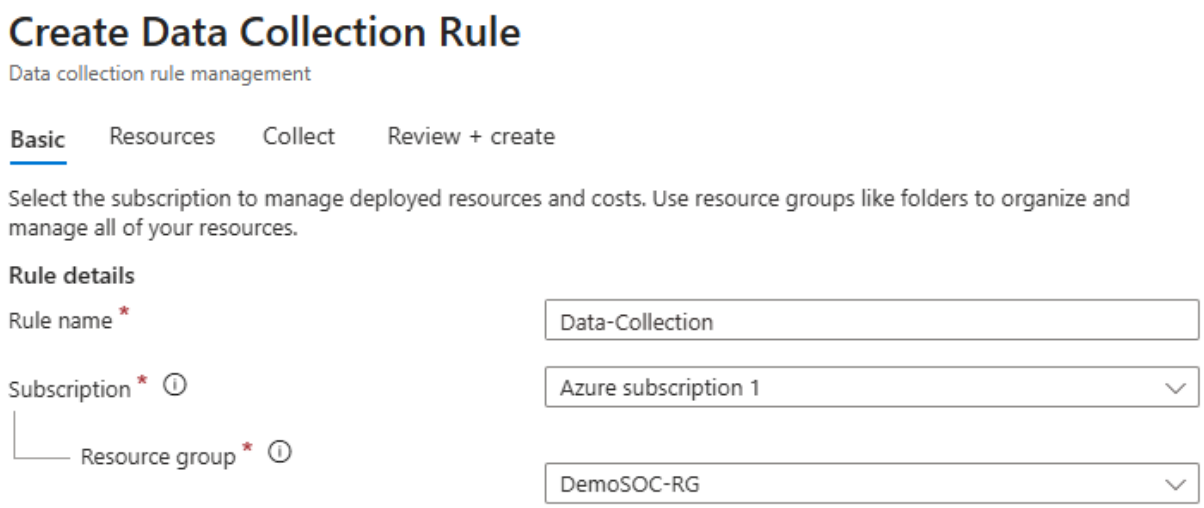

Fig 27

Select the device whose event log will be ingested

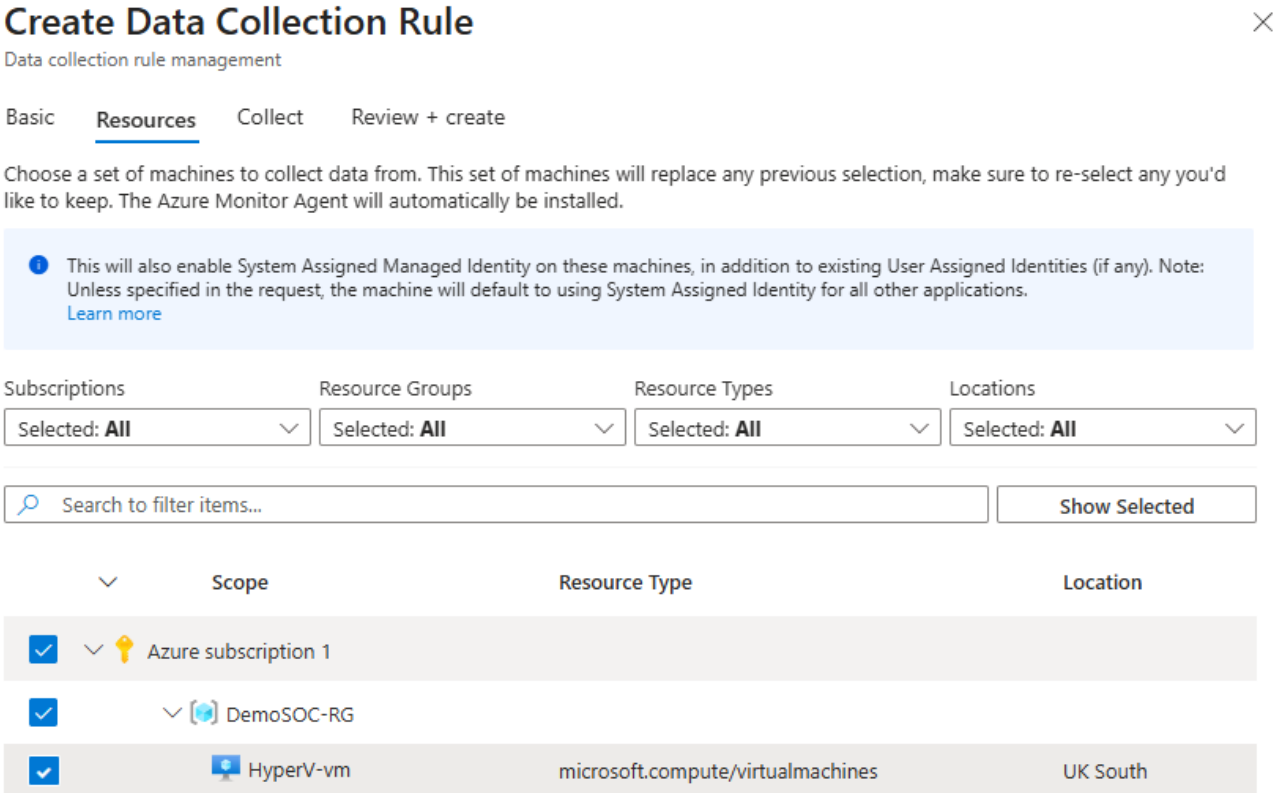

Fig 28

Ensure All security radio is checked.

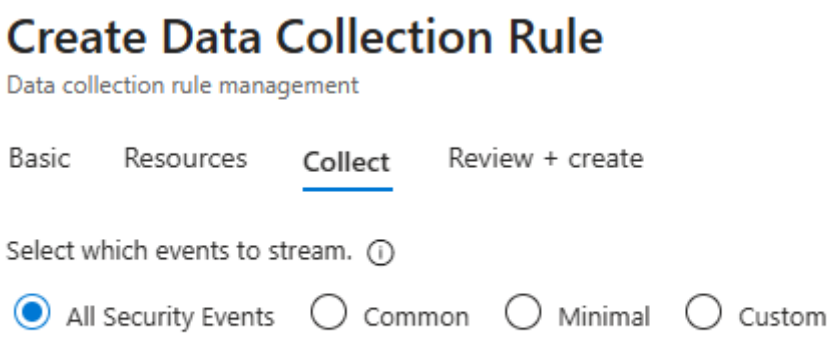

Fig 29

Review and create the rule.

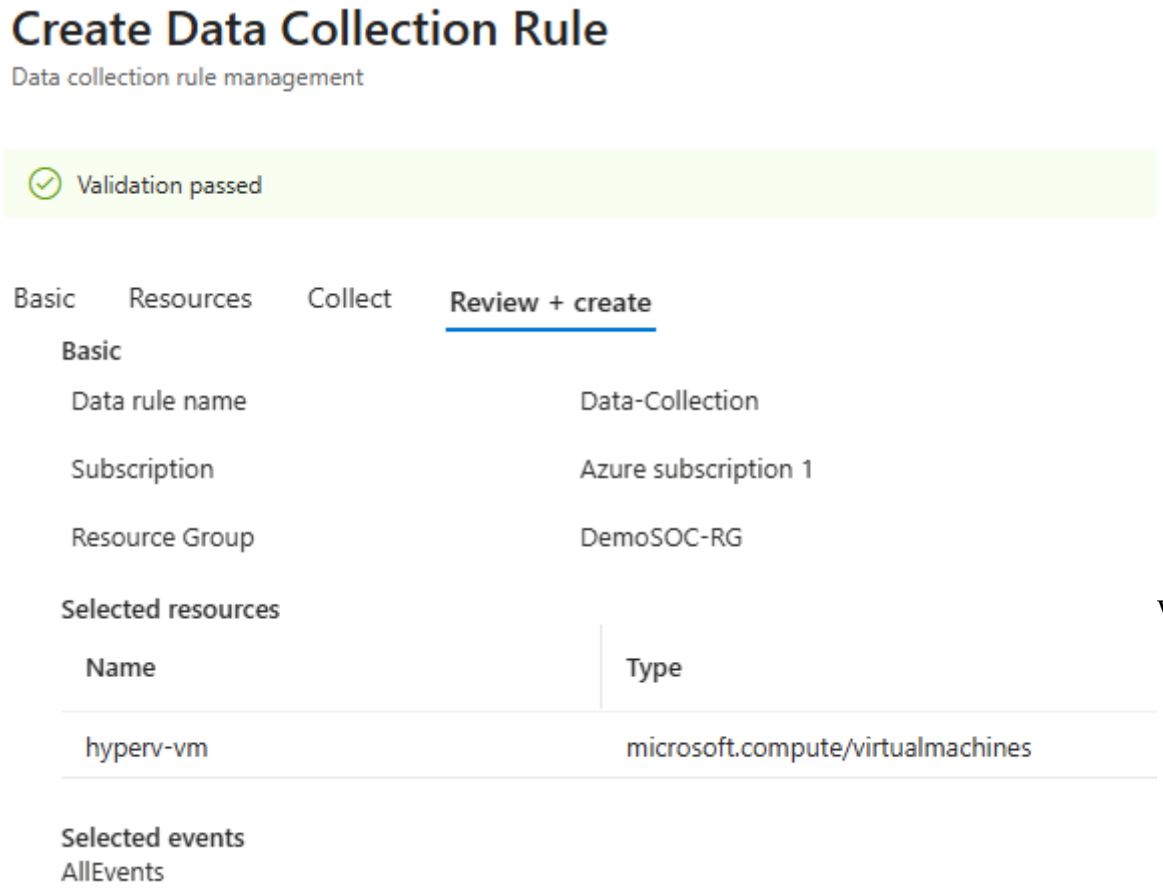

Fig 30

Give the provisioning of the agent time to complete.

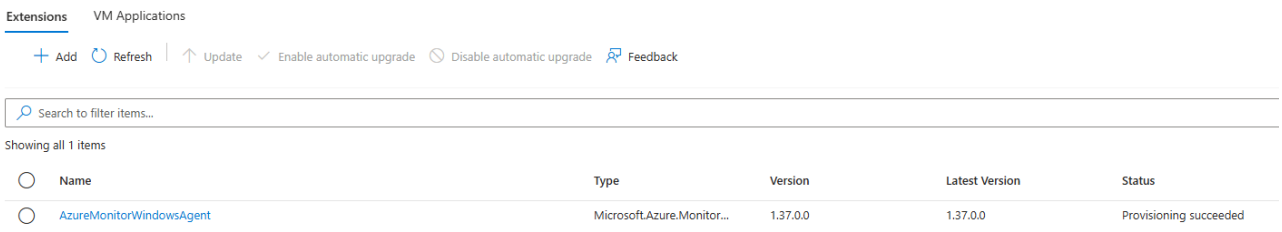

Fig 31

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

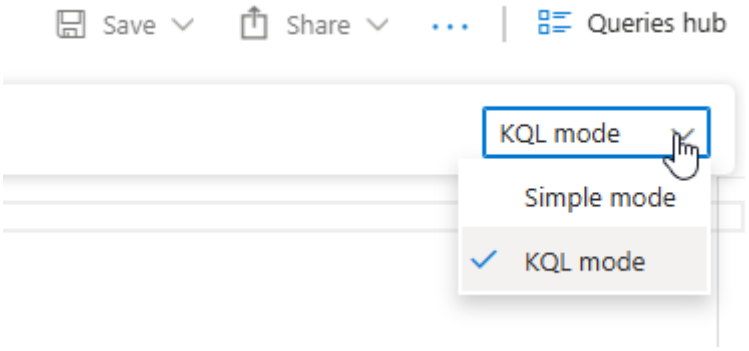

Fig 32

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

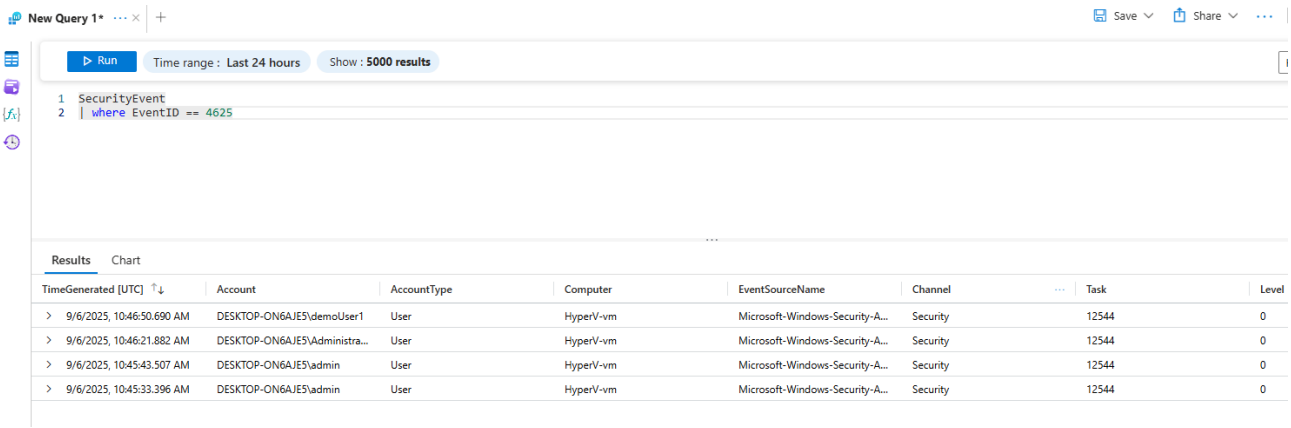

Fig 33

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

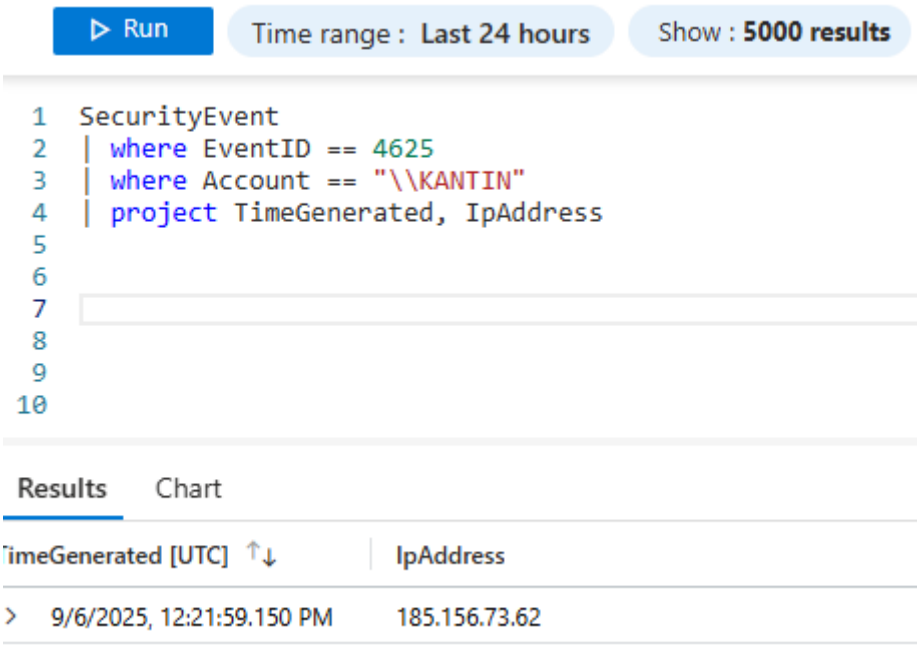

Fig 34

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

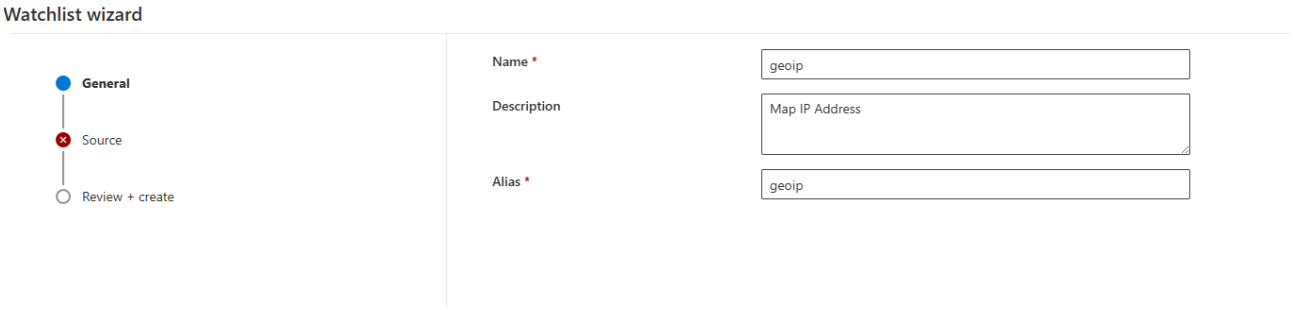

Fig 35

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

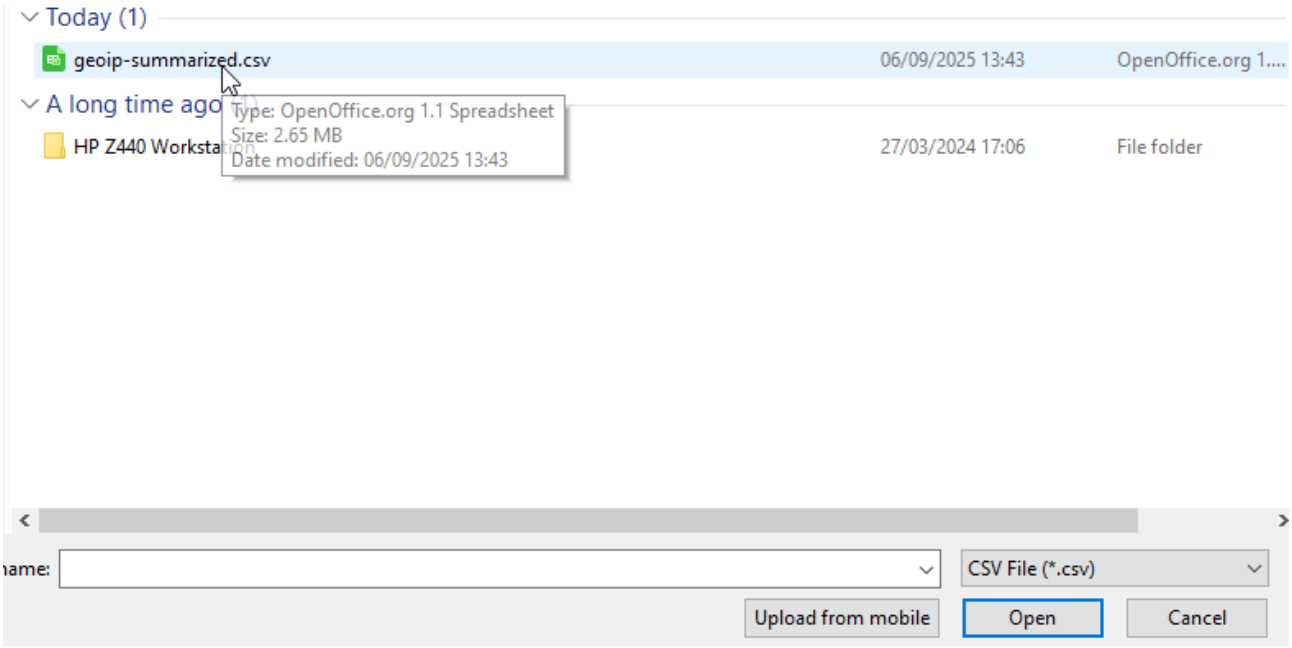

Fig 36

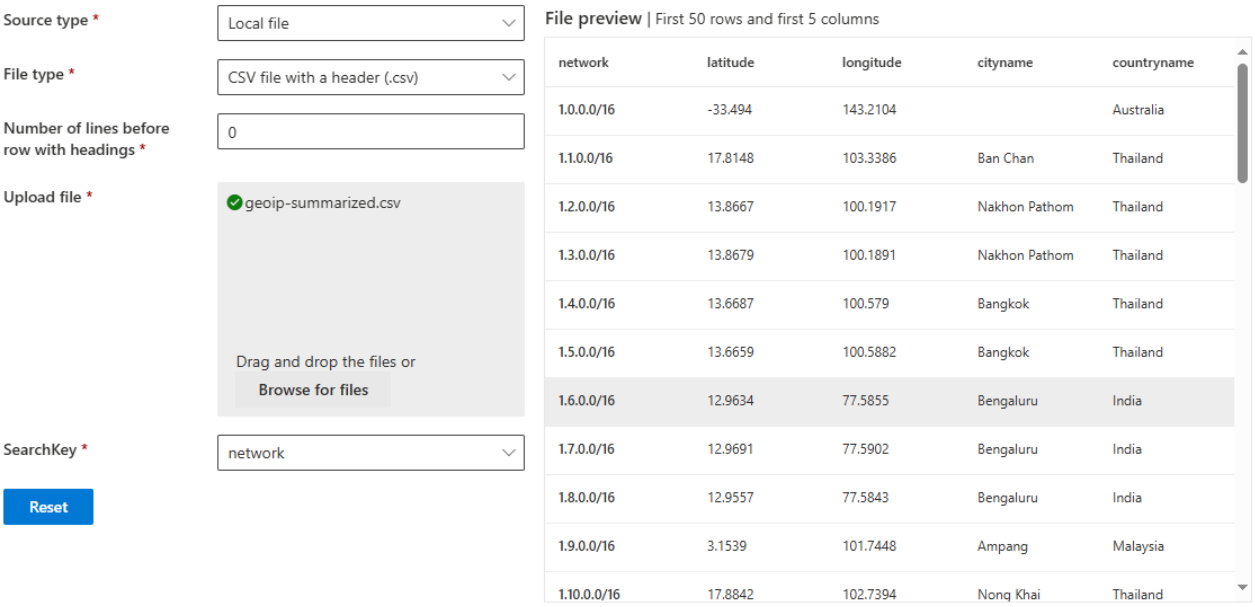

Fig 37

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

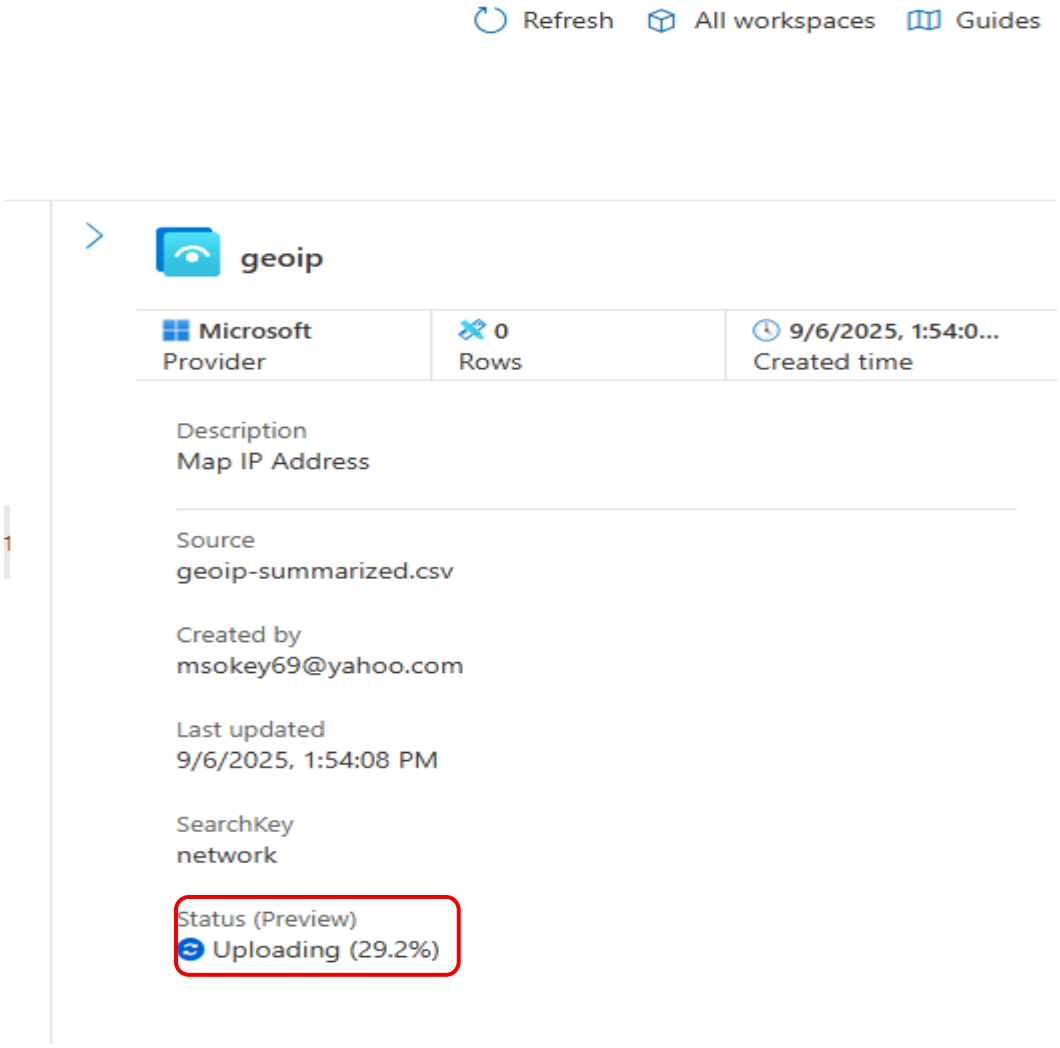
Refresh
All workspaces
Guides
geoip
Microsoft
Provider
0
Rows
9/6/2025, 1:54:0...
Created time
Description
Map IP Address
Source
geoip-summarized.csv
Created by
msokey69@yahoo.com
Last updated
9/6/2025, 1:54:08 PM
SearchKey
network
Status (Preview)
Uploading (29.2%)

Fig 38

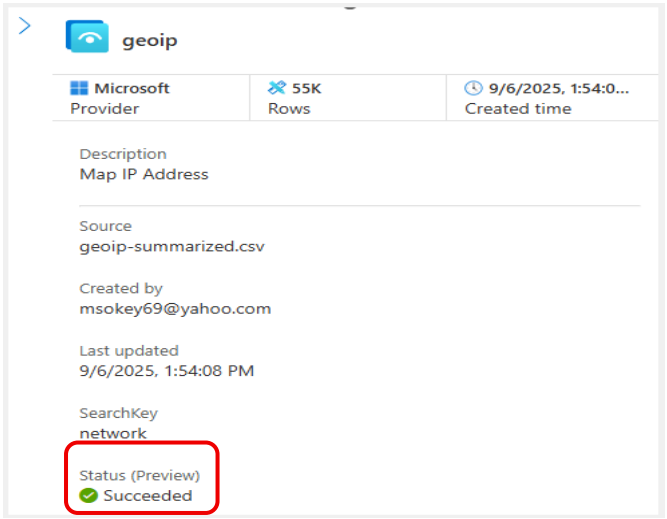
geoip
Microsoft
Provider
55K
Rows
9/6/2025, 1:54:0...
Created time
Description
Map IP Address
Source
geoip-summarized.csv
Created by
msokey69@yahoo.com
Last updated
9/6/2025, 1:54:08 PM
SearchKey
network
Status (Preview)
Succeeded

Fig 39

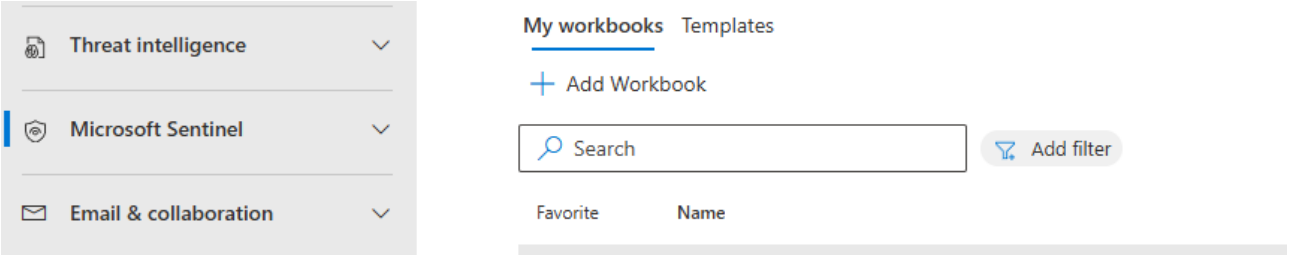

Fig 40

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

Fig 41

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

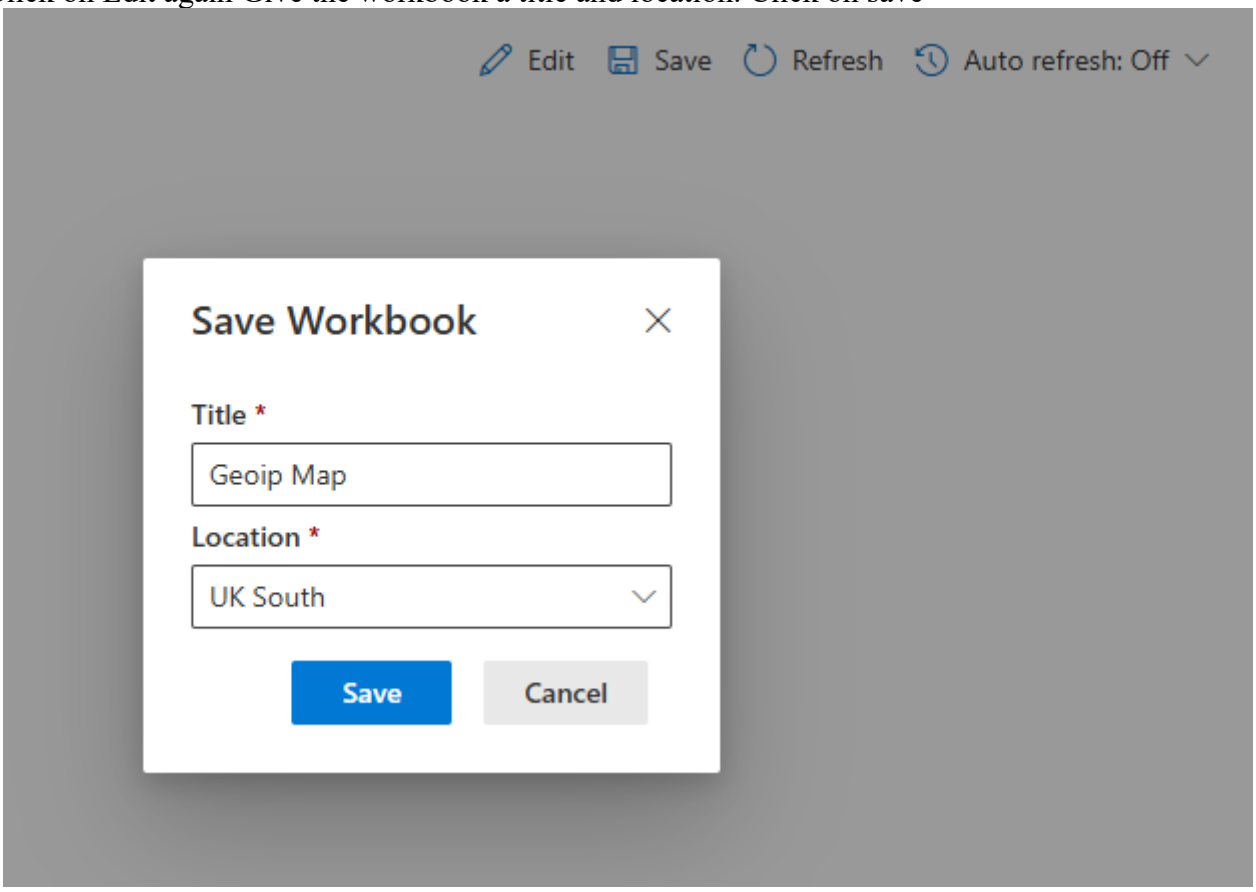

Fig 42

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 of where the attacking Ips are originating will be displayed.

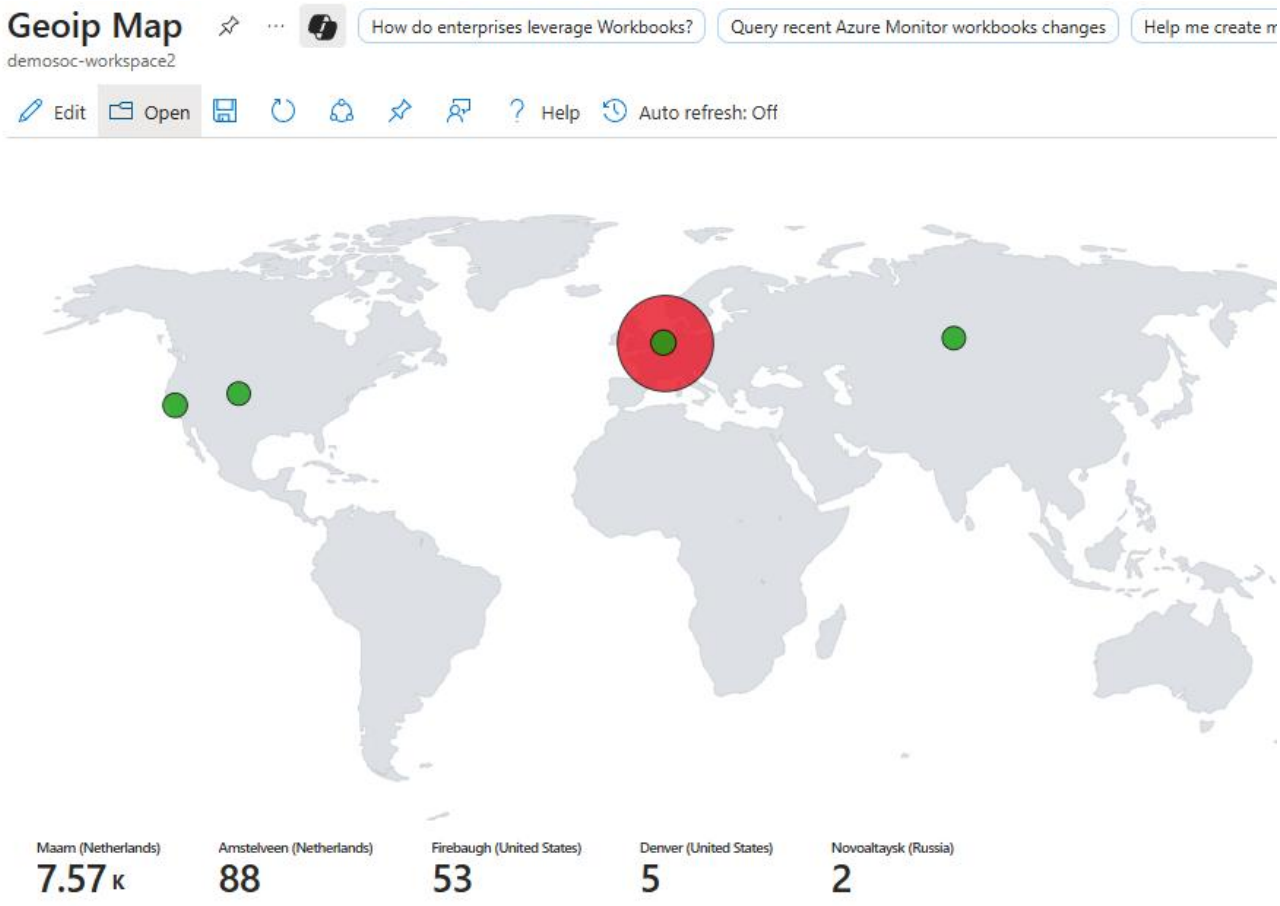

Fig 43

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 Microsoft Defender page. Under configuration, click on Analytics

Create a Scheduled Query.

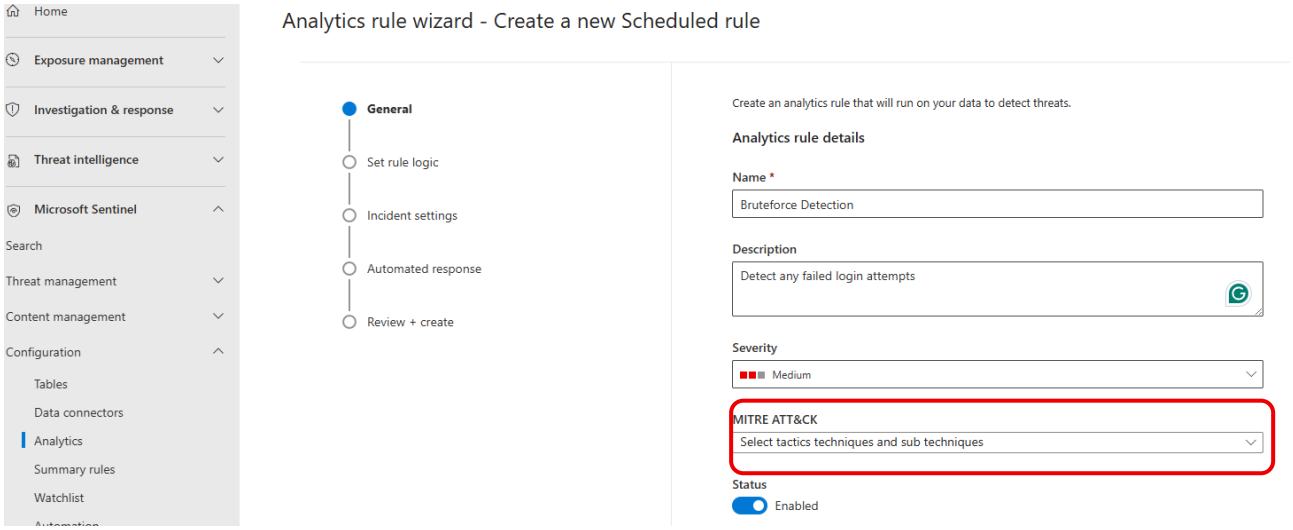

Fig 44

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

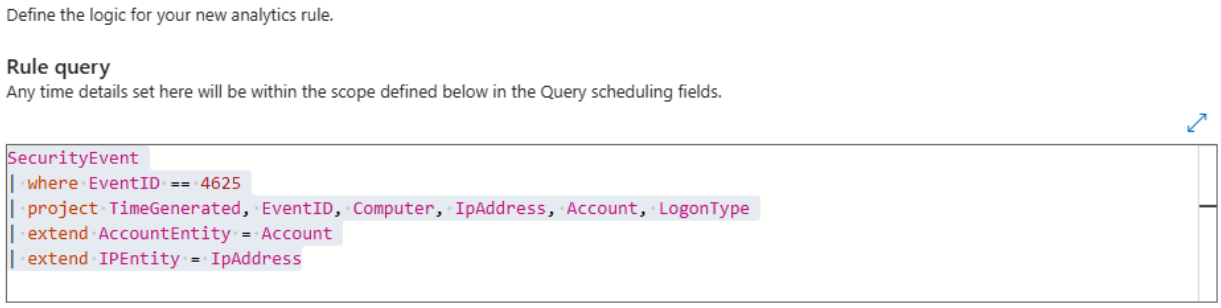

Fig 45

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

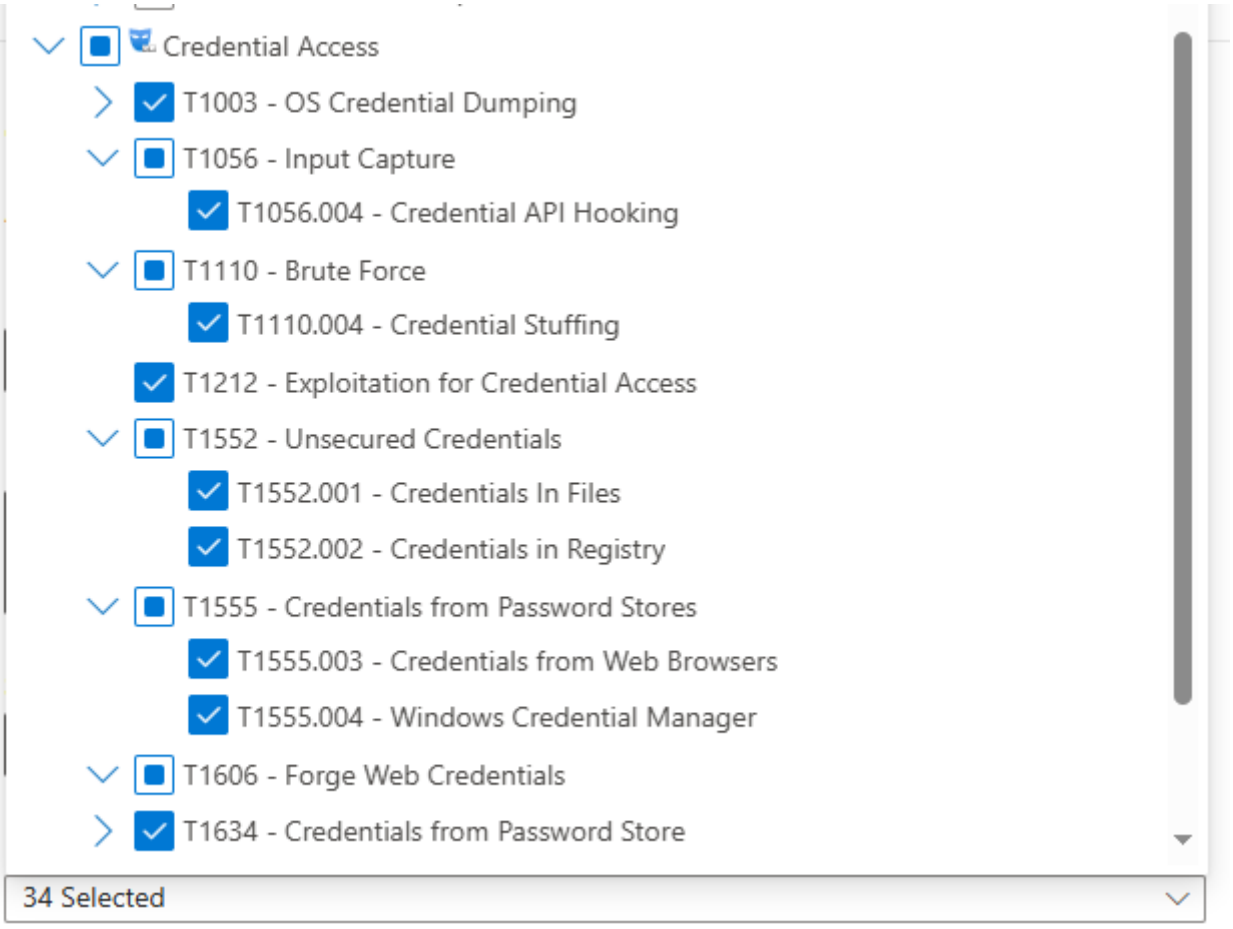

Fig 46

Set how often the rule will run.

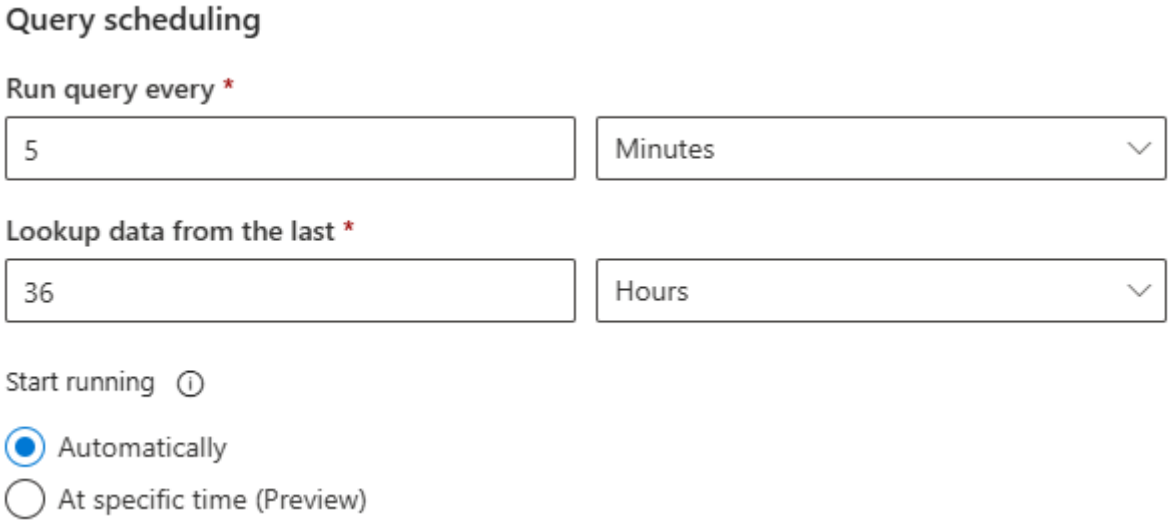

Fig 47

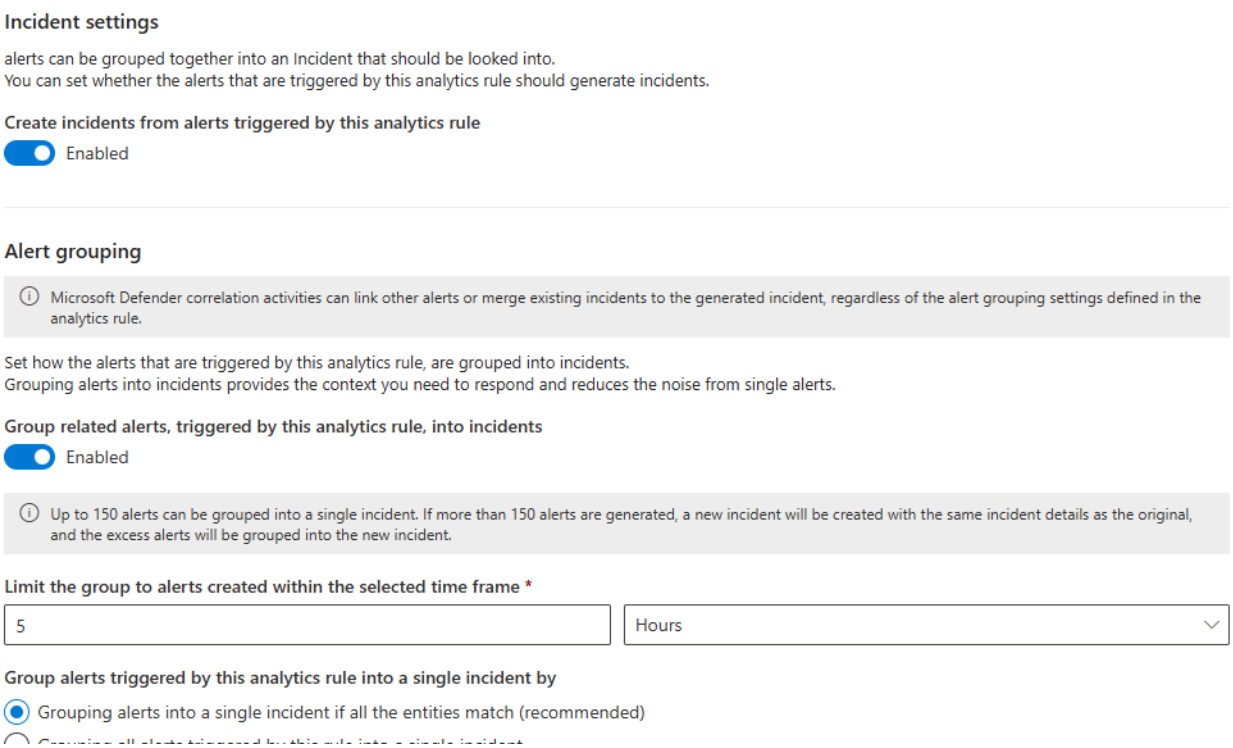

Fig 48

Enable Alert grouping

After a while, an Incident will be created

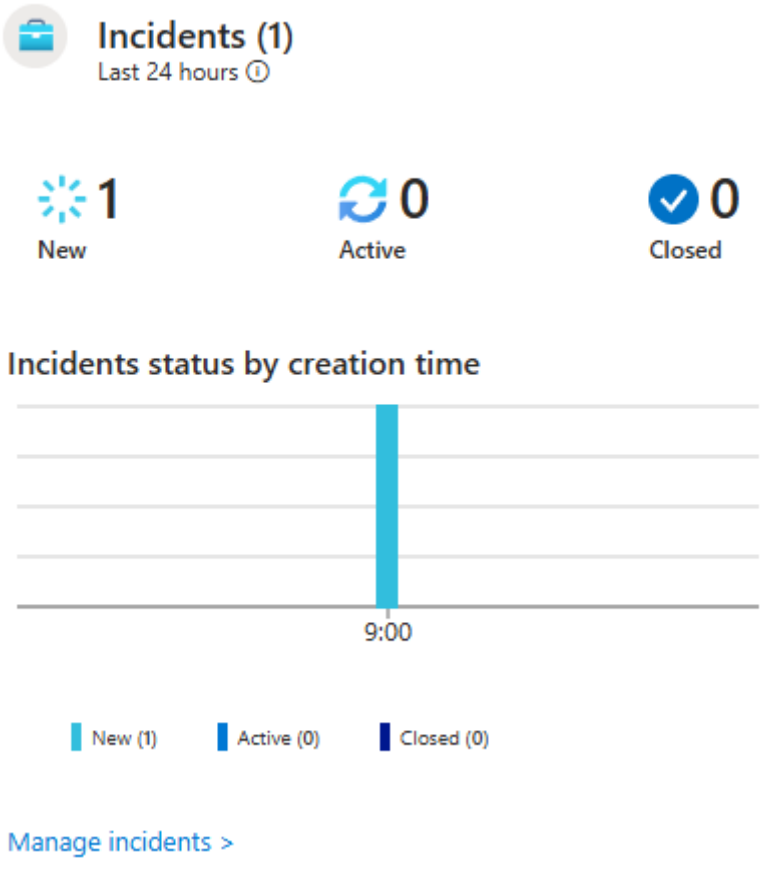

Fig 49

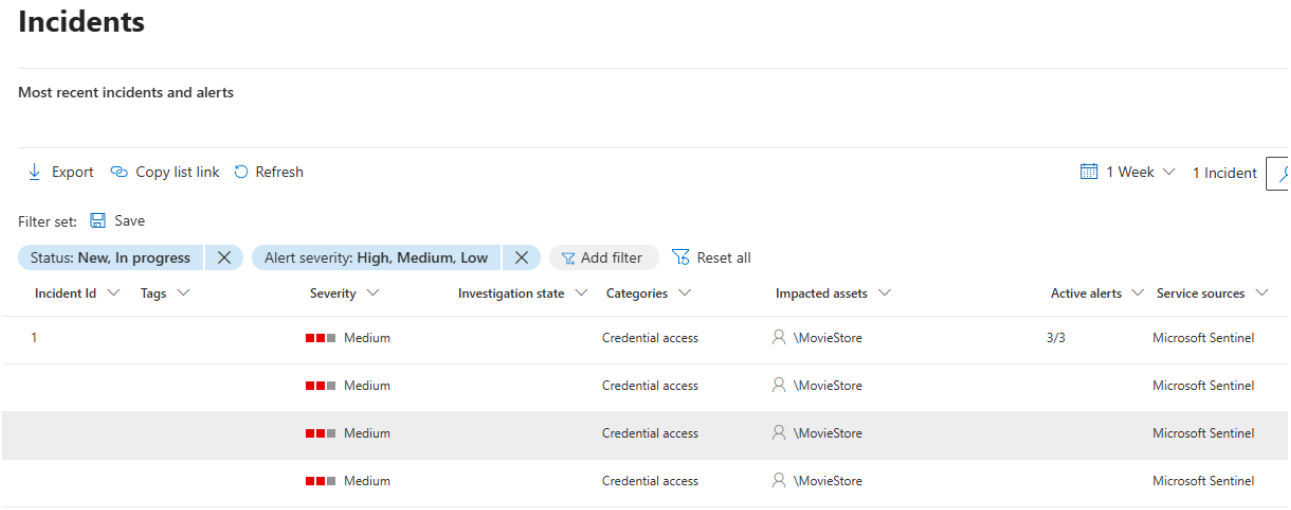
Incidents
Most recent incidents and alerts
Export
Copy list link
Refresh
1 Week
1 Incident
Filter set:
Save
Status: New, In progress
Alert severity: High, Medium, Low
Add filter
Reset all
Incident Id
Tags
Severity
Investigation state
Categories
Impacted assets
Active alerts
Service sources
1
Medium
Credential 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

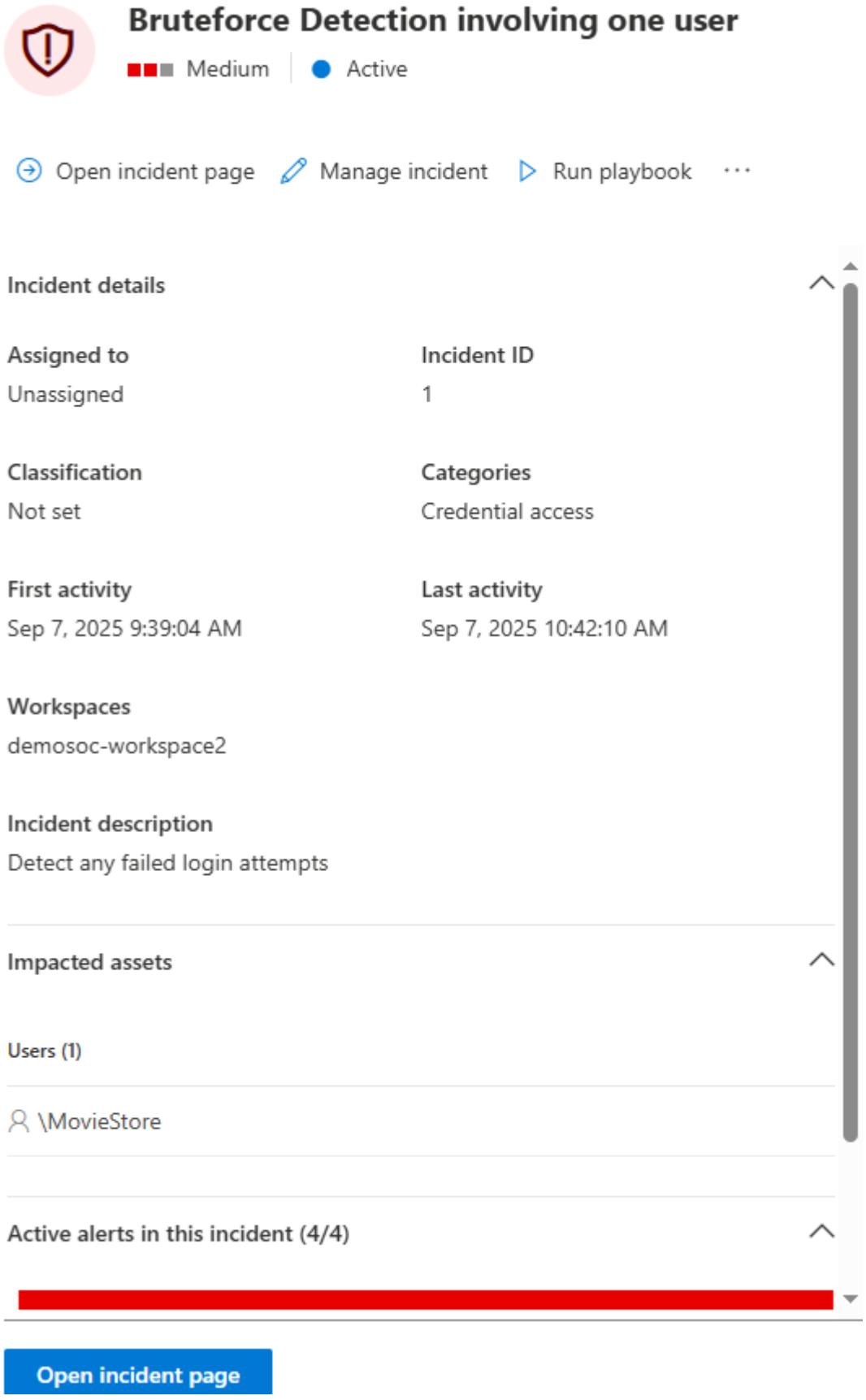
Bruteforce Detection involving one user
Medium
Active
Open incident page
Manage incident
Run playbook
Incident details
Assigned to
Unassigned
Incident ID
1
Classification
Not set
Categories
Credential access
First activity
Sep 7, 2025 9:39:04 AM
Last activity
Sep 7, 2025 10:42:10 AM
Workspaces
demosoc-workspace2
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.

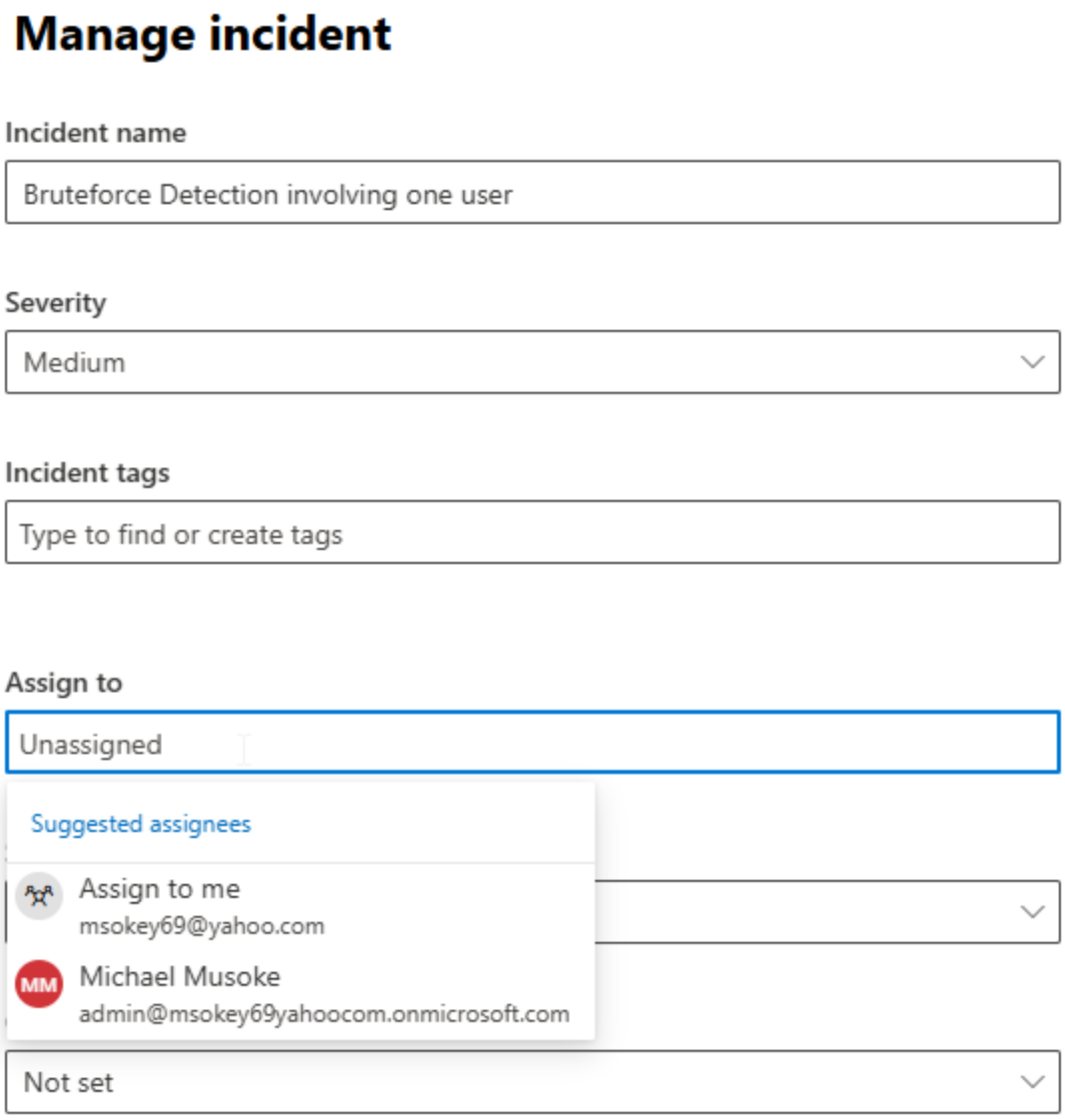

Fig 52

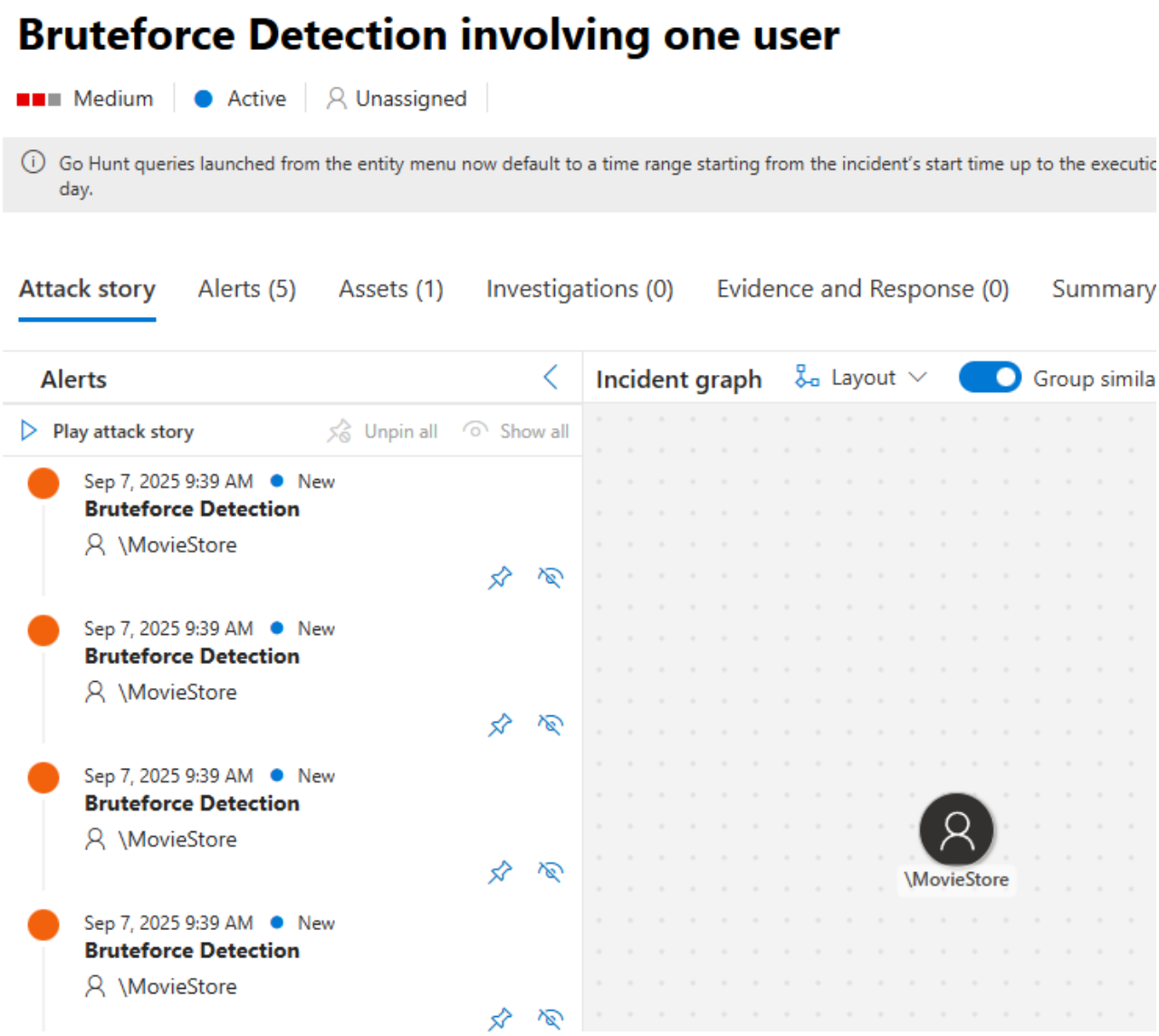
Bruteforce Detection involving one user
Medium
Active
Unassigned
Go Hunt queries launched from the entity menu now default to a time range starting from the incident's start time up to the executic
day.
Attack story
Alerts (5)
Assets (1)
Investigations (0)
Evidence and Response (0)
Summary
Alerts
Play attack story
Unpin all
Show all
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
Incident graph
Layout
Group simila
\MovieStore

Fig 54

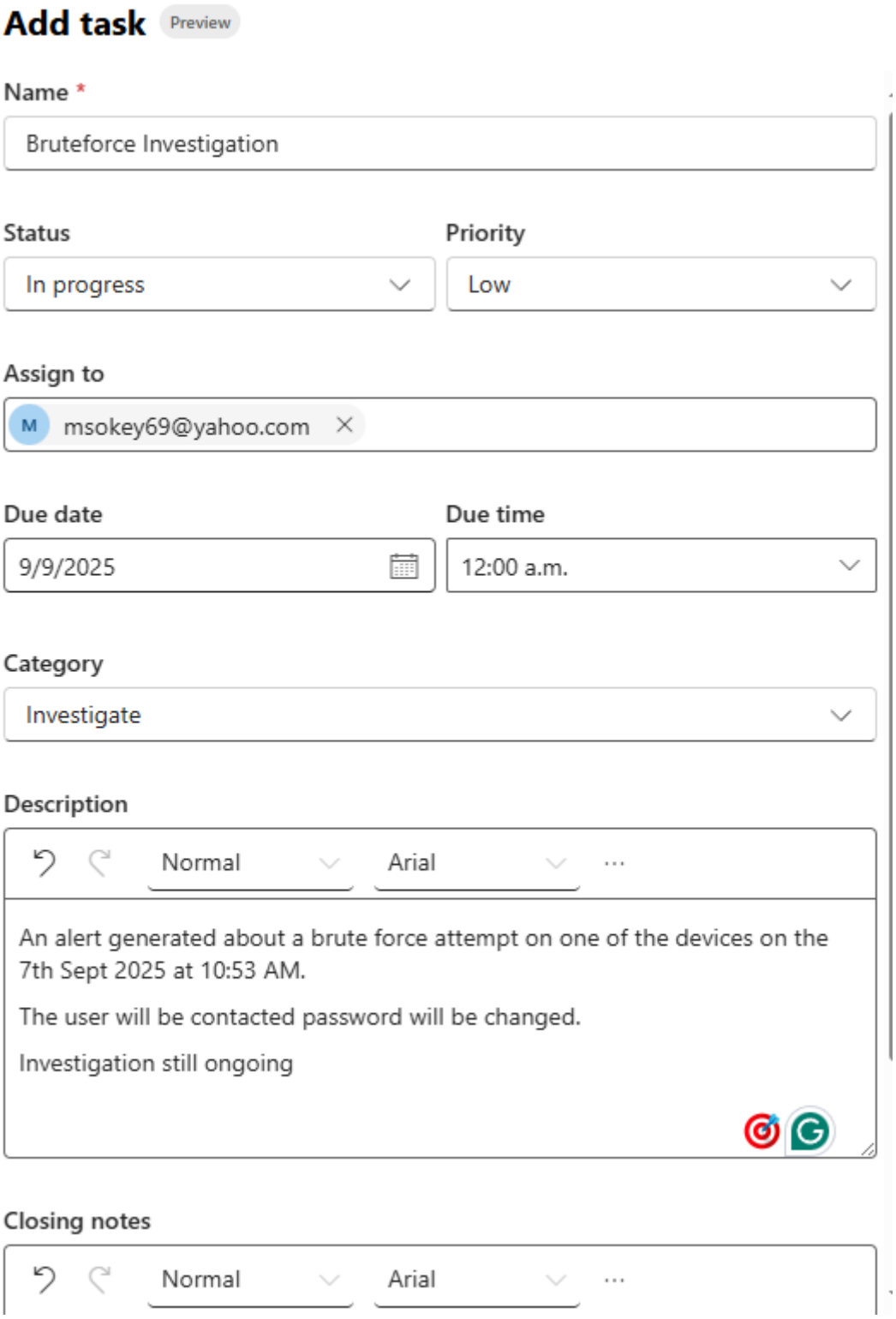
Add task
Preview
Name *
Bruteforce Investigation
Status
In progress
Priority
Low
Assign to
M
msokey69@yahoo.com
Due date
9/9/2025
Due time
12:00 a.m.
Category
Investigate
Description
Normal
Arial
An alert generated about a brute force attempt on one of the devices on the 7th Sept 2025 at 10:53 AM.
The user will be contacted password will be changed.
Investigation still ongoing
Closing notes
Normal
Arial

Fig 55

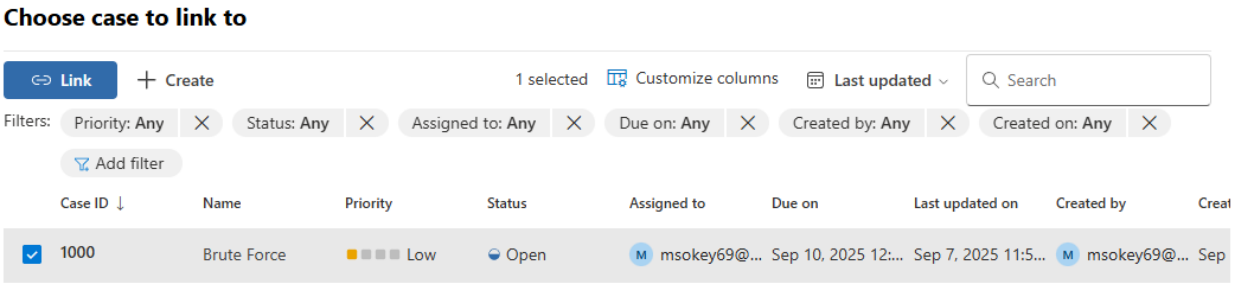

Fig 56

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

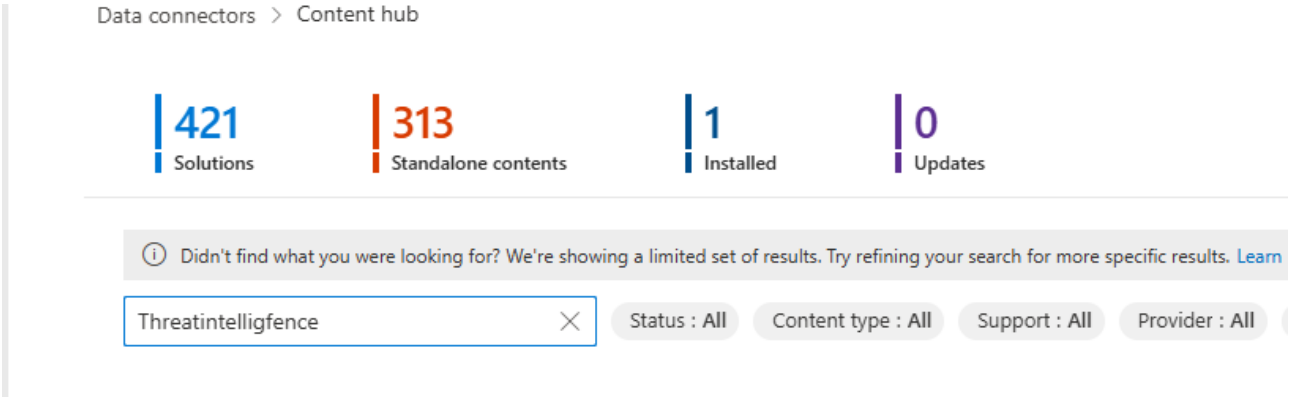

Fig 57

Select the first instance of Threat Intelligence

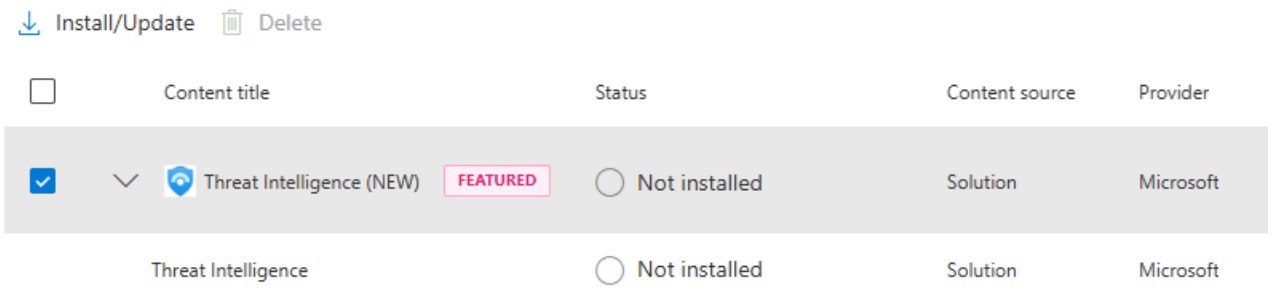

Fig 58

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

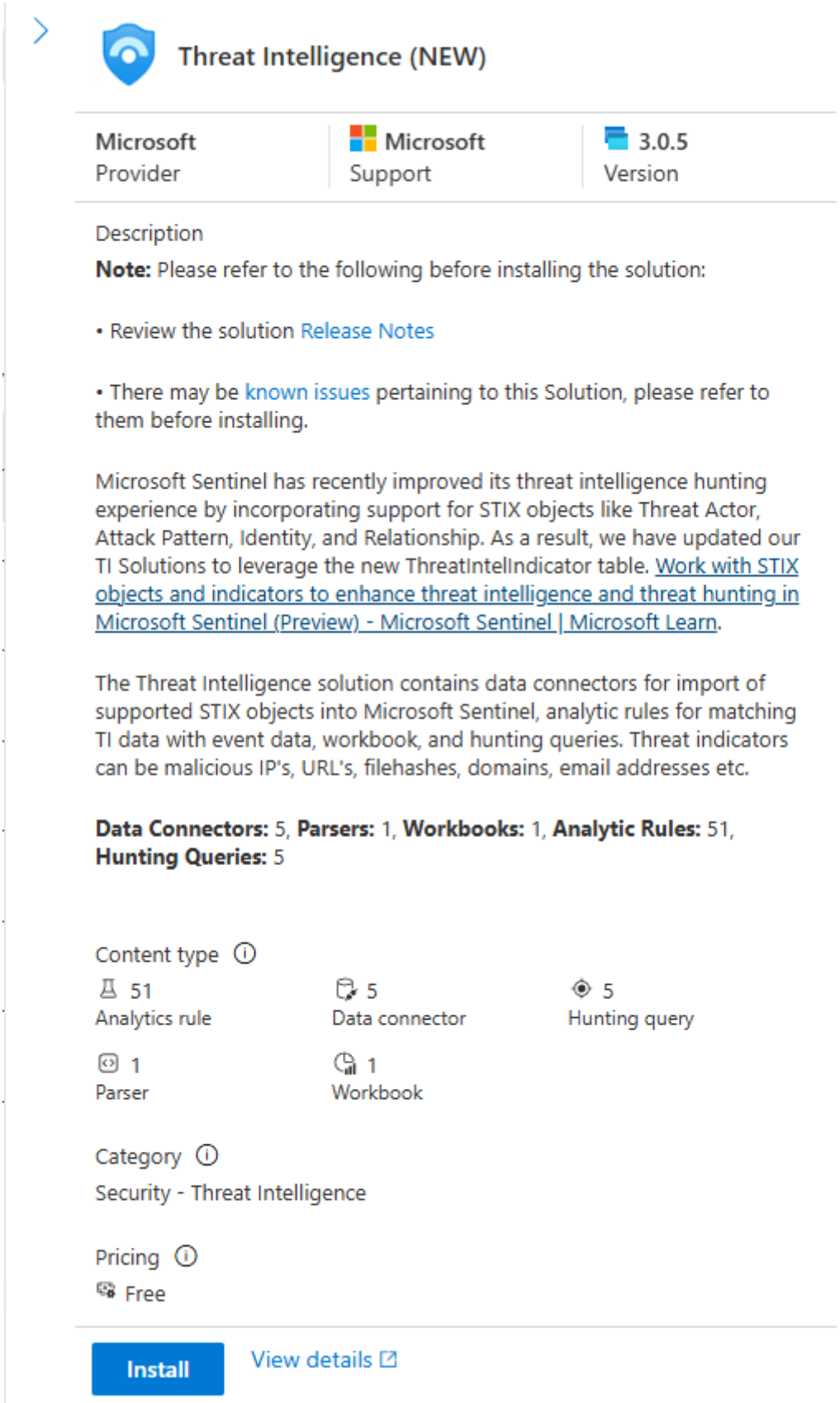

Fig 59

Click on Manage after the installation is completed

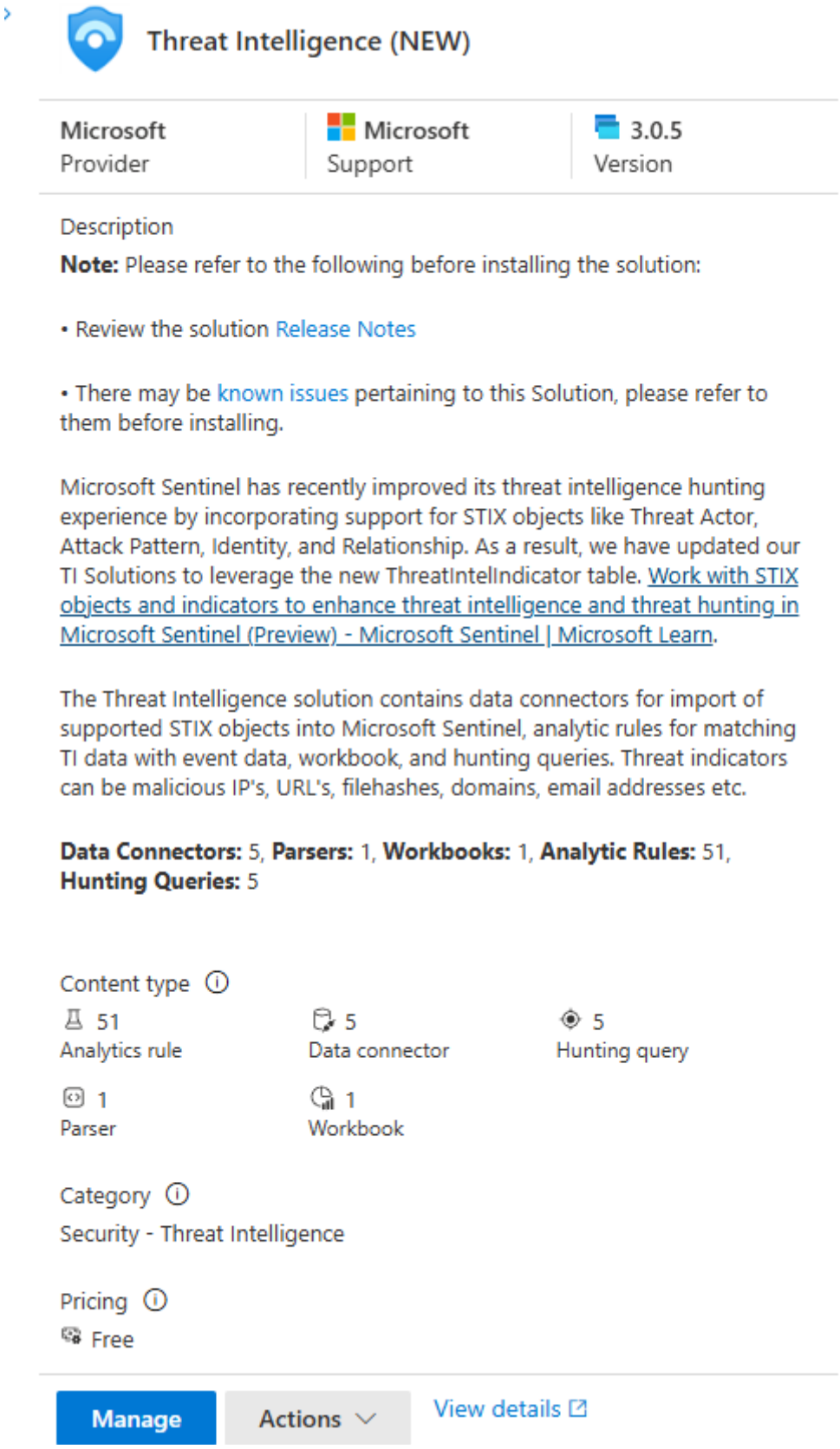

Fig 60

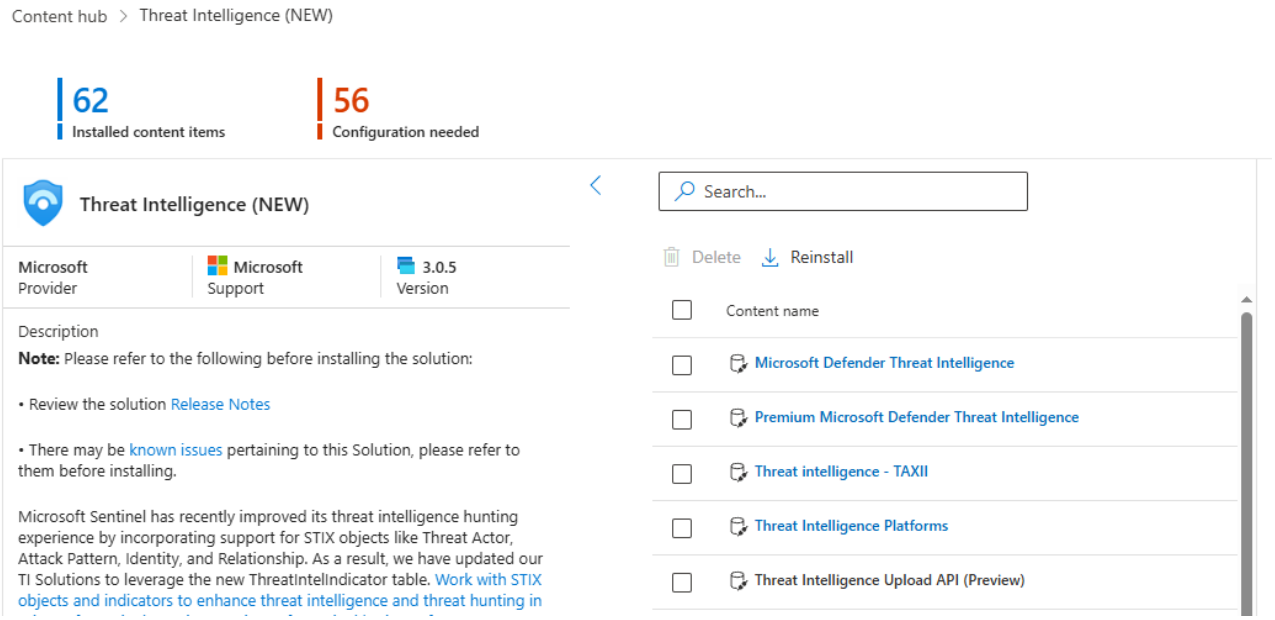

Fig 61

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

To receive data from Pulsedive and account is required.

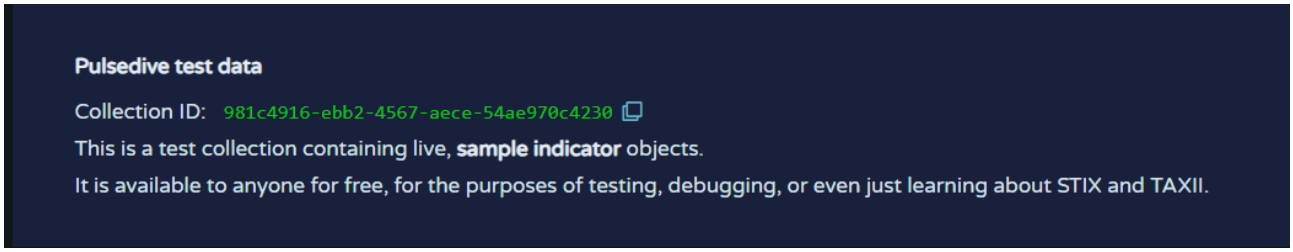

Fig 63

Fig 64

On the Threat intelligence page, click on Open connector page

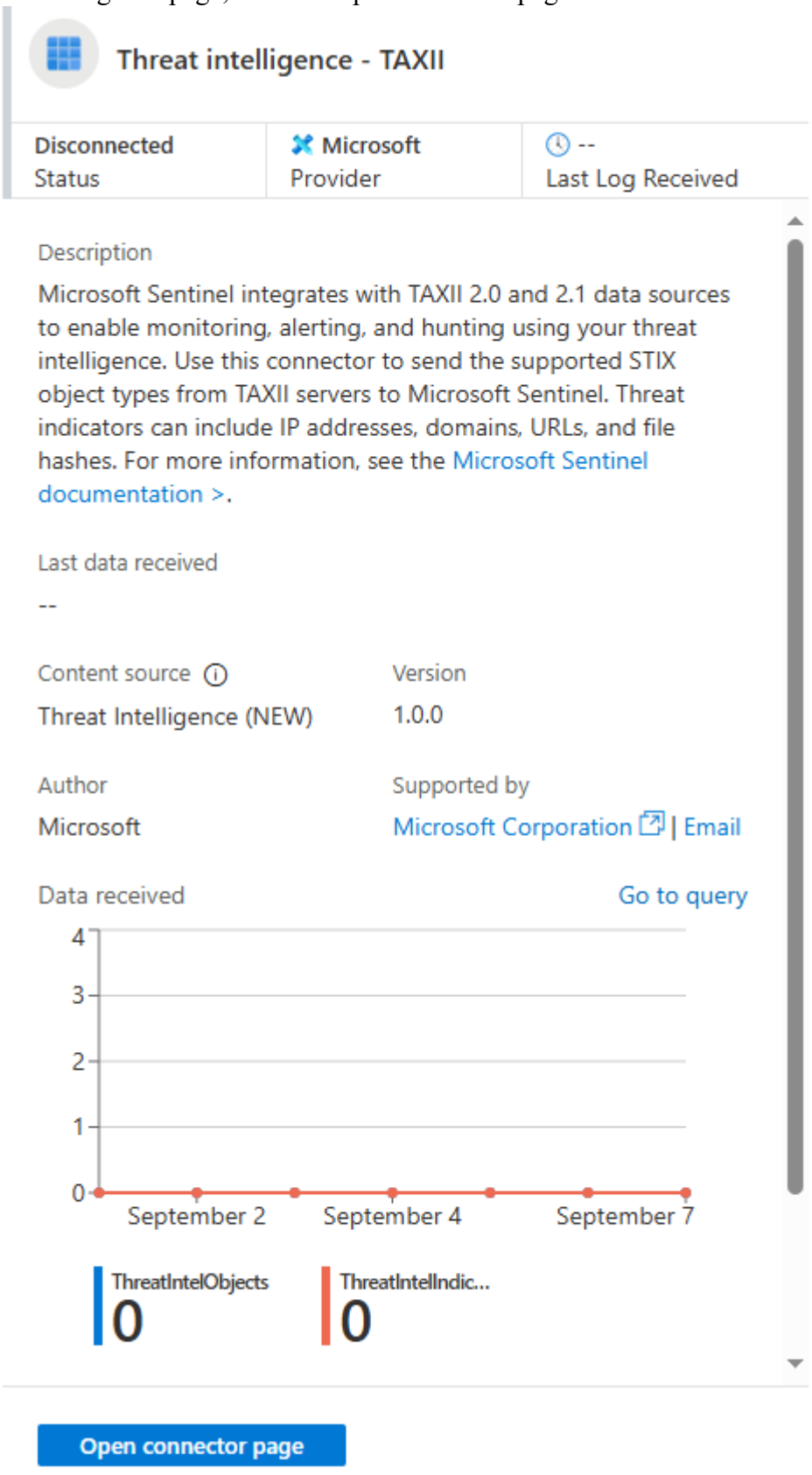

Fig 62

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

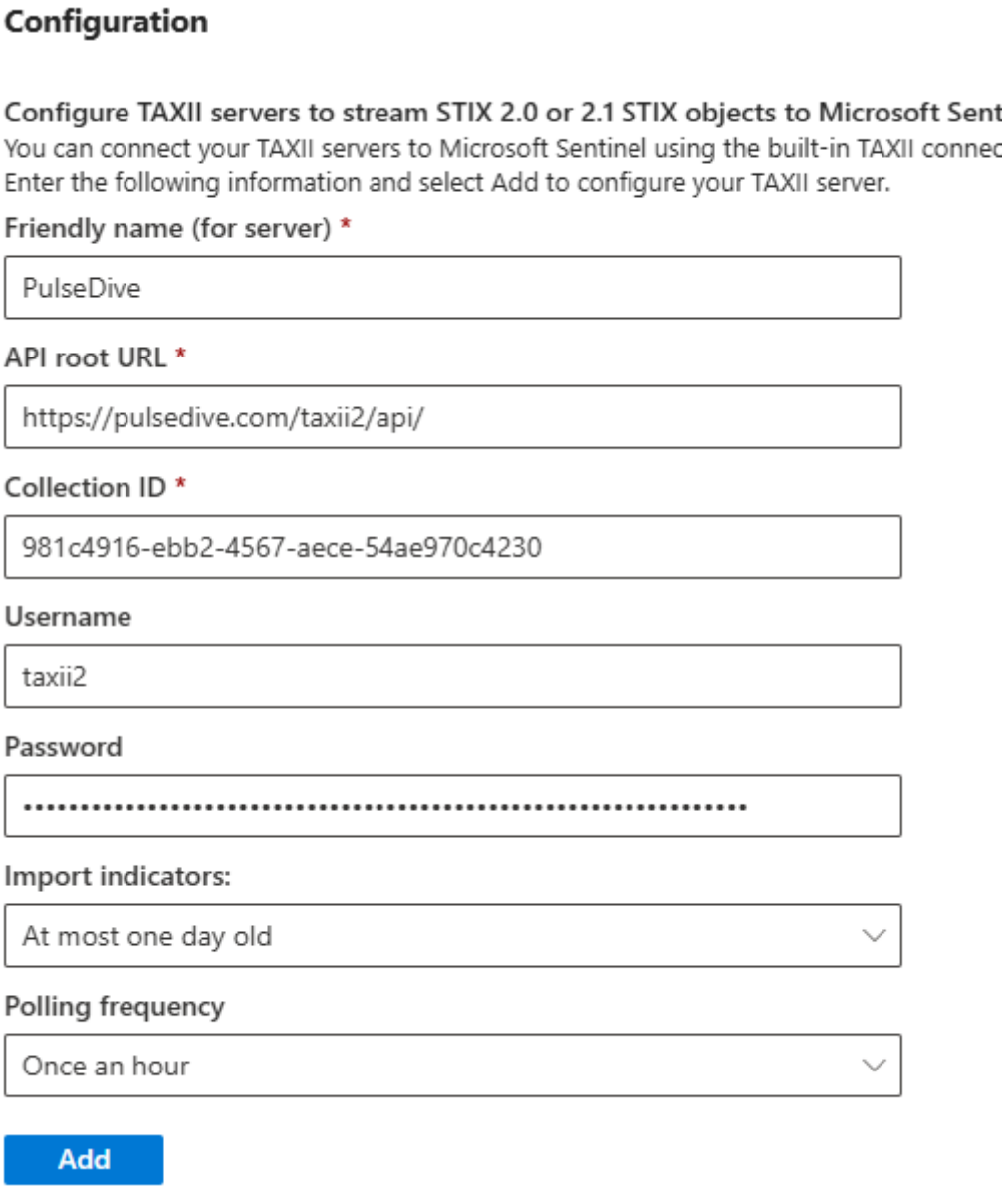

Fig 65

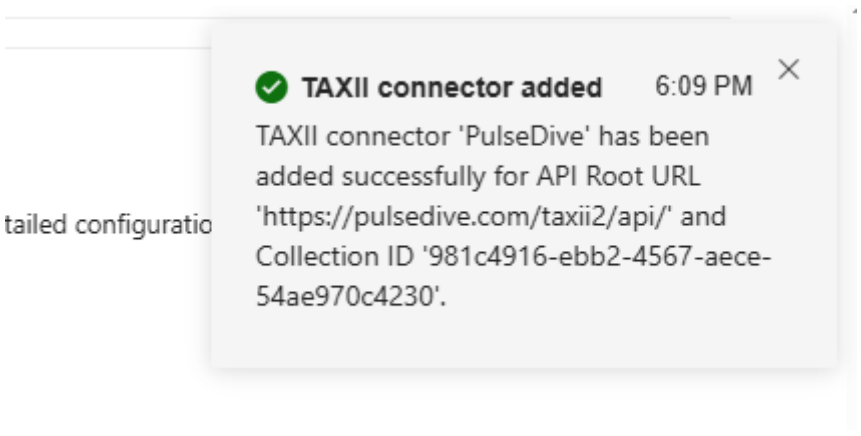

Fig 66

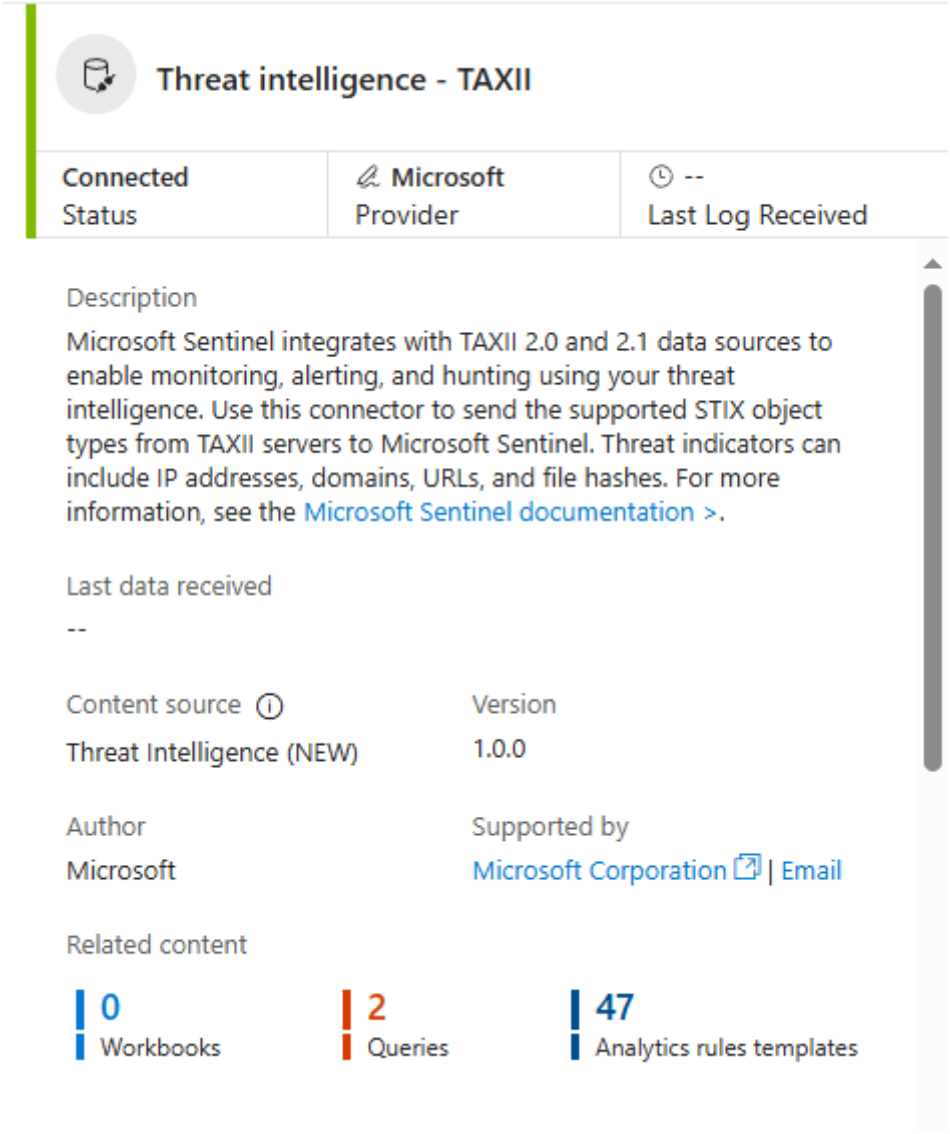
Threat intelligence - TAXII
Connected
Status
Microsoft
Provider
--
Last Log Received
Description
Microsoft Sentinel integrates with TAXII 2.0 and 2.1 data sources to enable monitoring, alerting, and hunting using your threat intelligence. Use this connector to send the supported STIX object types from 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
Threat Intelligence (NEW)
Version
1.0.0
Author
Microsoft
Supported by
Microsoft Corporation | Email
Related content
0
Workbooks
2
Queries
47
Analytics rules templates

Fig 67

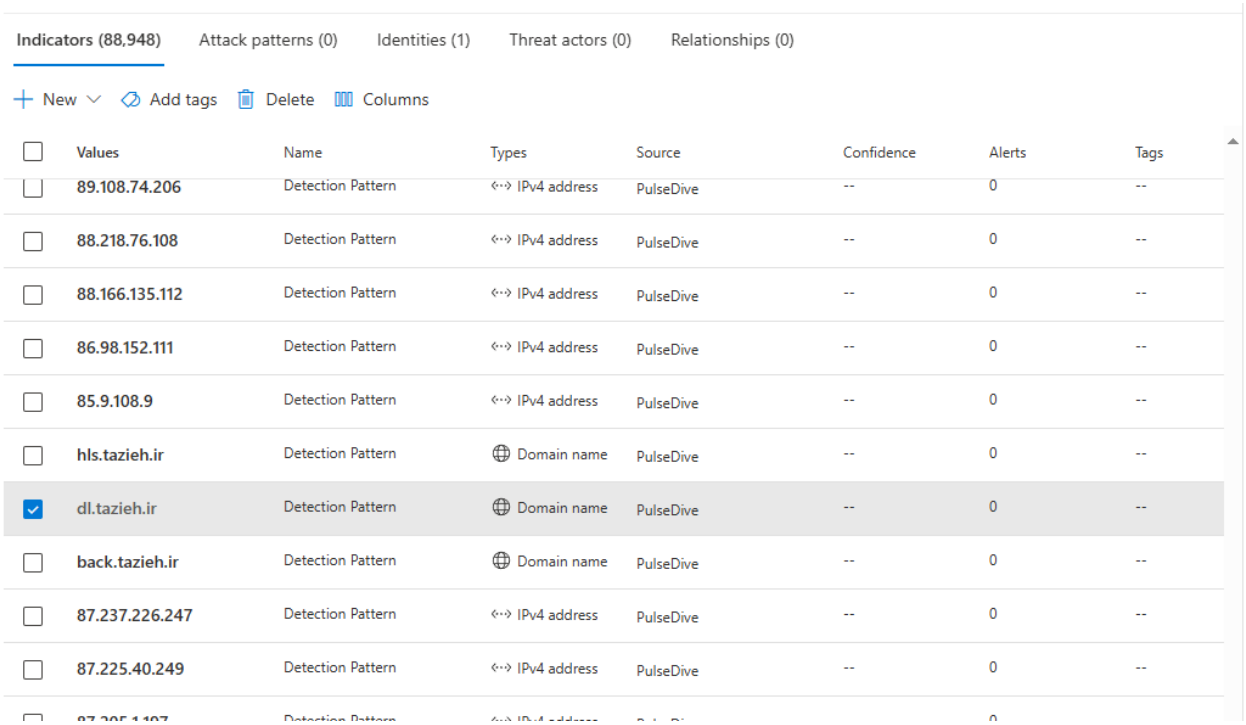
Indicators (88,948)
Attack patterns (0)
Identities (1)
Threat actors (0)
Relationships (0)
New
Add tags
Delete
Columns
Values
Name
Types
Source
Confidence
Alerts
Tags
89.108.74.206 Detection Pattern IPv4 address PulseDive -- 0 --
88.218.76.108 Detection Pattern IPv4 address PulseDive -- 0 --
88.166.135.112 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 --

Fig 68

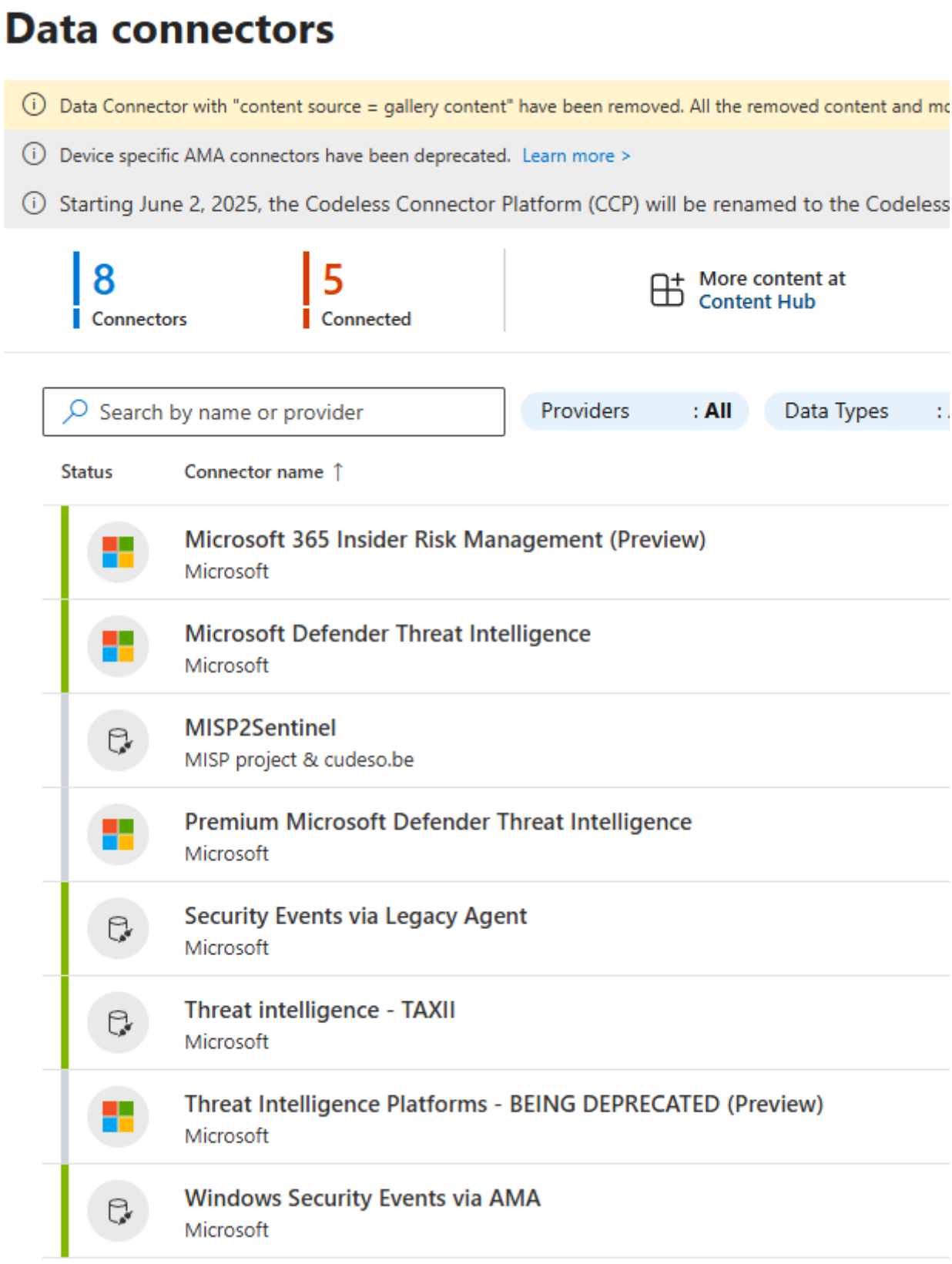
Data connectors
Data Connector with "content source = gallery content" have been removed. All the removed content and mo
Device specific AMA connectors have been deprecated. Learn more >
Starting June 2, 2025, the Codeless Connector Platform (CCP) will be renamed to the Codeless
8
Connectors
5
Connected
More content at
Content Hub
Search by name or provider
Providers : All
Data Types :
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

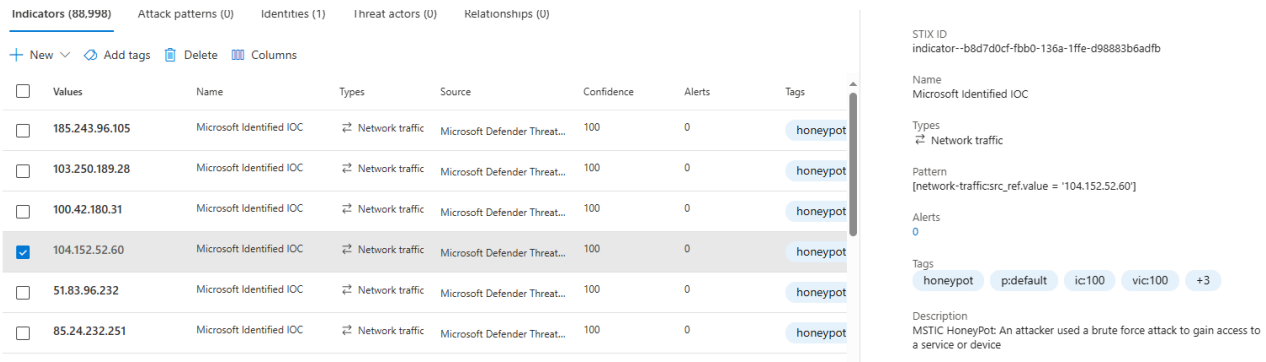

Fig 70

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.