

## 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

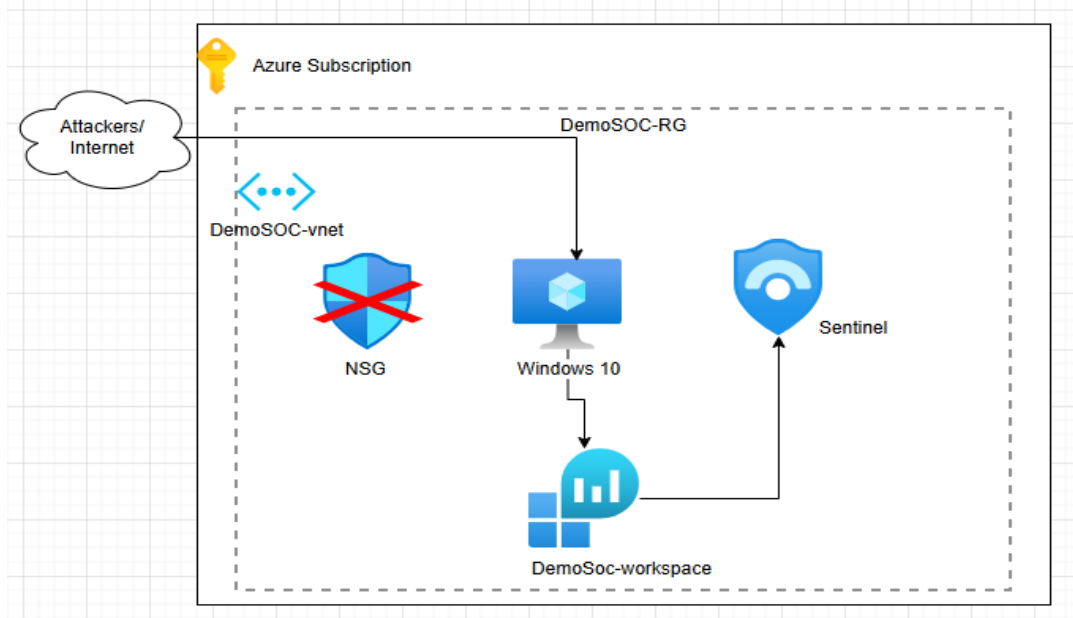


Fig 1

## 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.

## 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 * ⓘ	<div>Azure subscription 1</div>
Resource group name * ⓘ	<div>DemoSOC-RG</div>
Region * ⓘ	<div>(Europe) UK South</div>

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 *	<div>Azure subscription 1</div>
Resource group *	<div>DemoSOC-RG</div> <div><a href="#">Create new</a></div>

### Instance details

Virtual network name *	<div>DemSoc-vnet</div>
Region * ⓘ	<div>(Europe) UK South</div>

[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 *	<div>Azure subscription 1</div>
Resource group *	<div>DemoSOC-RG</div> <div><a href="#">Create new</a></div>

### Instance details

Virtual machine name *	<div>HyperV-vm</div>
Region *	<div>(Europe) UK South</div> <div><a href="#">Deploy to an Azure Extended Zone</a></div>
Availability options	<div>Availability zone</div>

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 ⓘ ☐  
 ⓘ Hibernation is not supported by the size that you have selected. Choose a size that is compatible with Hibernation 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 VM

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)
	<a href="#">Edit virtual network</a>
Subnet * ⓘ	(New) snet-uksouth-1
	<a href="#">Edit subnet</a> 10.0.1.0 - 10.0.1.255 (256 addresses)
Public IP ⓘ	(new) HyperV-vm-ip
	<a href="#">Create new</a>
NIC network security group ⓘ	<input type="radio"/> None <input checked="" type="radio"/> Basic <input type="radio"/> Advanced
Public inbound ports * ⓘ	<input type="radio"/> None <input checked="" type="radio"/> 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

+ Create

Switch to classic

Reservations

Manage view

Refresh

Export to CSV

Open query

Assign tags

Start

Restart

Stop

Delete

Ser

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

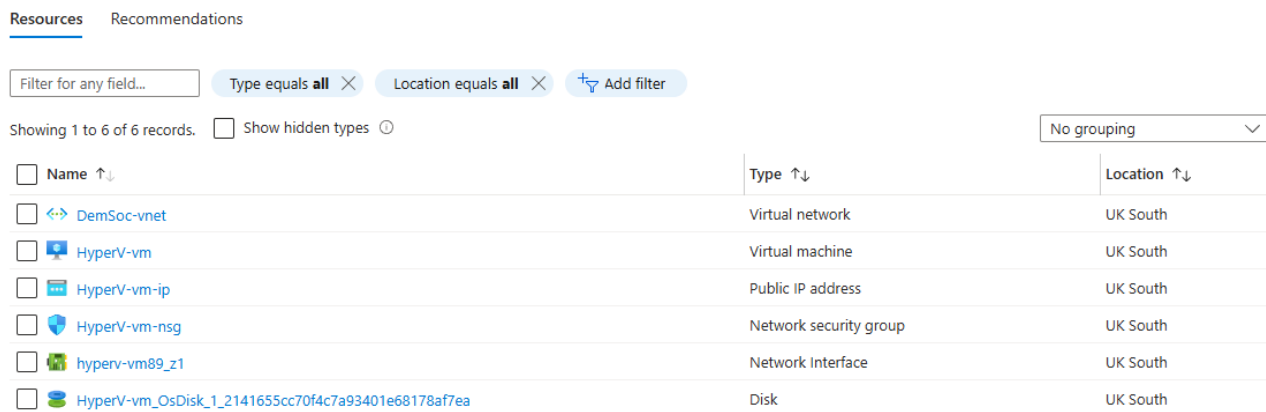
Location equals all

+ Add filter

<input type="checkbox"/>	Name ↑	Subscription	Resource Group	Location	Status	Operating system	Size	Public IP address
<input type="checkbox"/>	<div><div></div><div>HyperV-vm</div></div>	<div><div>...</div><div>Azure subscription 1</div></div>	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.

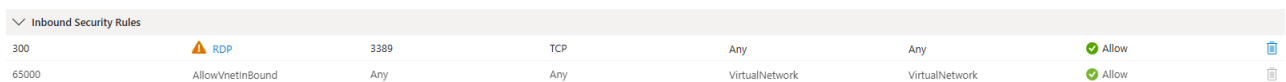


Resources			Recommendations
Filter for any field...			Type equals all × Location equals all × Add filter
Showing 1 to 6 of 6 records. <input type="checkbox"/> Show hidden types			No grouping
<input type="checkbox"/> Name ↑↓	Type ↑↓	Location ↑↓	
<input type="checkbox"/> DemSoc-vnet	Virtual network	UK South	
<input type="checkbox"/> HyperV-vm	Virtual machine	UK South	
<input type="checkbox"/> HyperV-vm-ip	Public IP address	UK South	
<input type="checkbox"/> HyperV-vm-nsg	Network security group	UK South	
<input type="checkbox"/> hyperv-vm89_z1	Network Interface	UK South	
<input type="checkbox"/> 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

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.

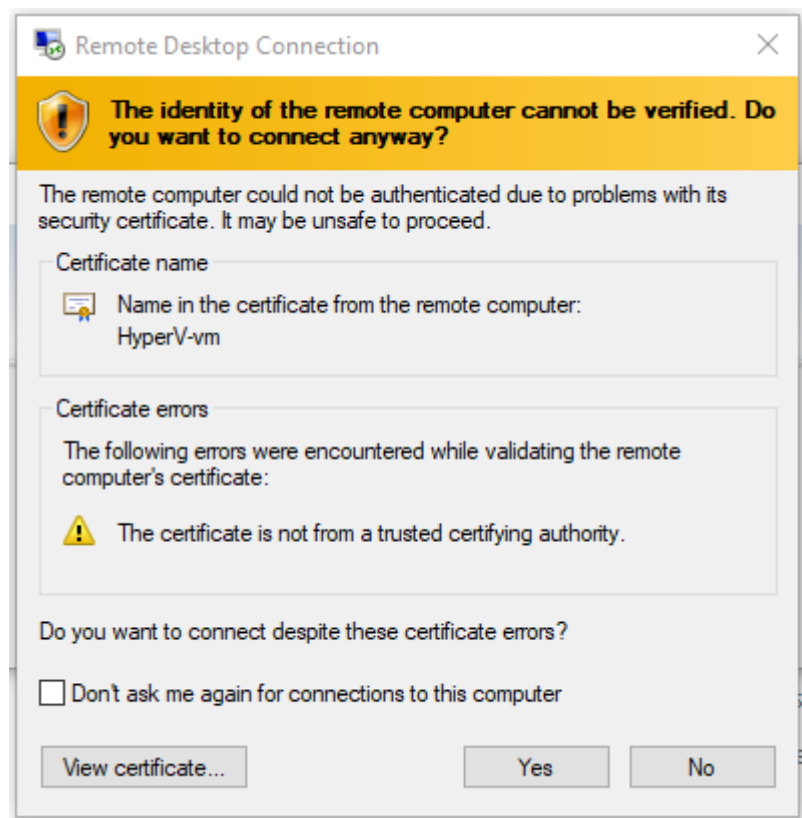


Fig 11

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

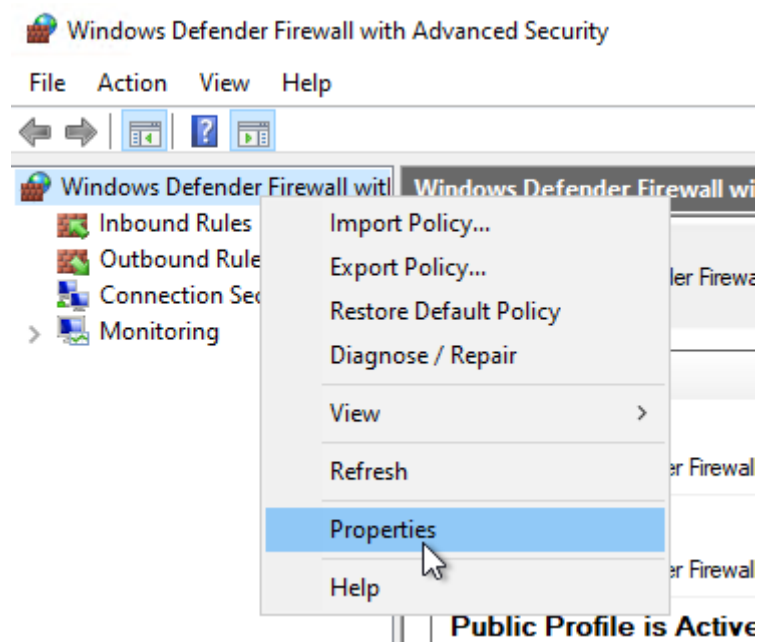


Fig 12



Disable the firewall state in all the tabs.

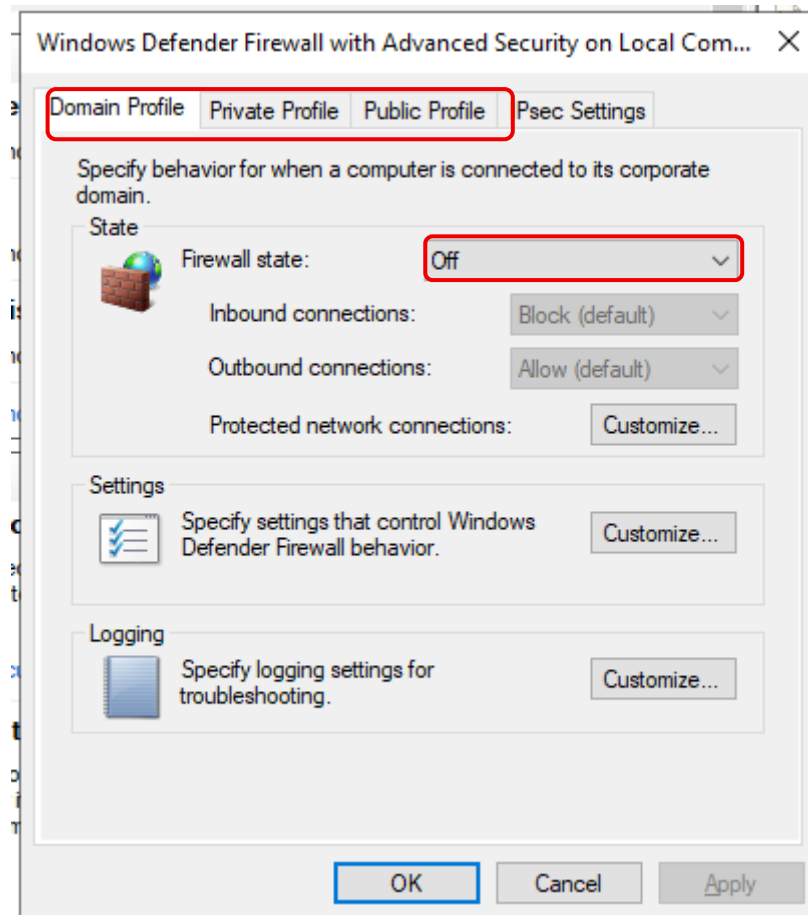


Fig 13

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.

```
C:\> 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

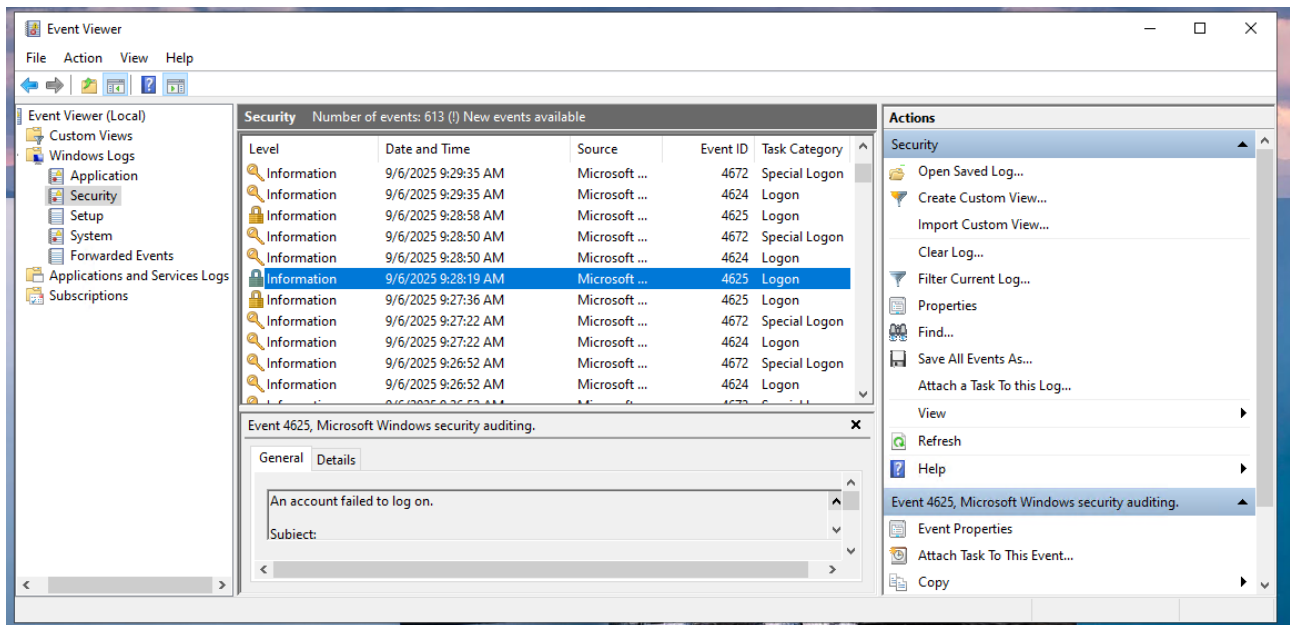


Fig 15

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

**Basics** Tags Review + Create

**i** 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

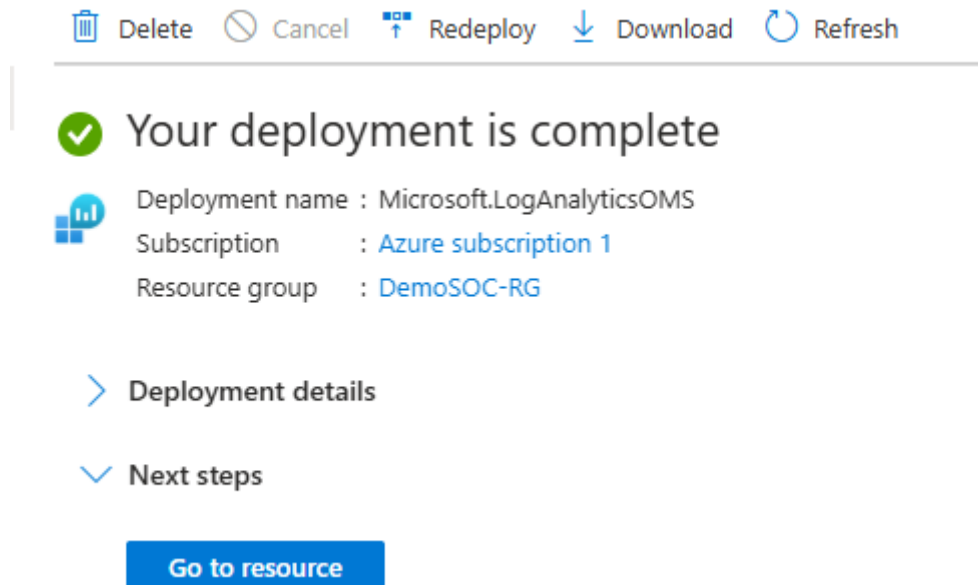


Fig 17

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

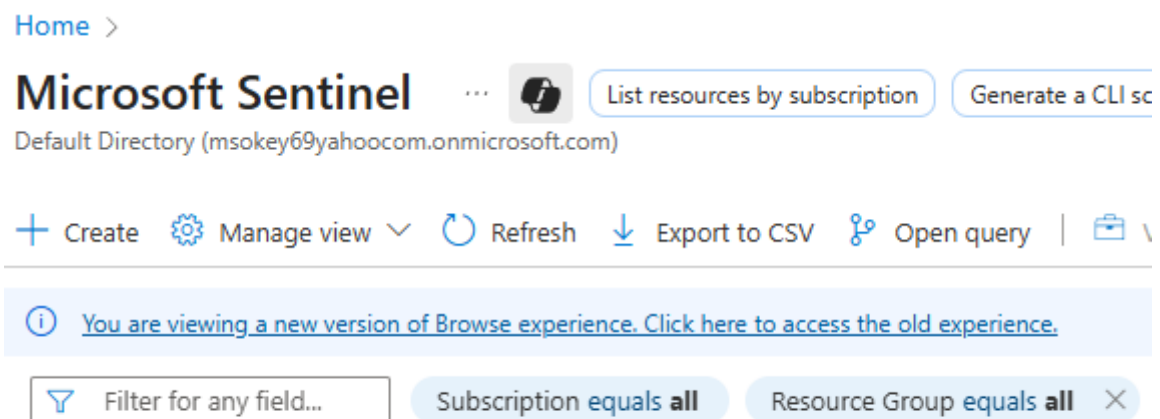


Fig 18

## Add Microsoft Sentinel to a workspace ...

+ Create a new workspace    ↻ Refresh

🔗 Microsoft Sentinel offers a 31-day free trial. See [Microsoft Sentinel pricing](#) for more details.

ℹ️ 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

« Documentation

---

**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.](#)

**OK**


---

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'

Refresh

Install/Update

Delete

SIEM Migration

Guides & Feedback

General

Overview

Logs

Guides

Search

Threat management


Content management

**Content hub**


Repositories

Community


Configuration

 **419**


Solutions

 **320**

Standalone contents

 **0**

Installed

 **0**

Updates

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

Status : All

Content type : All




<input type="checkbox"/>	Content title	Status
<input type="checkbox"/>	<div><div>▼</div><div> SlashNext Security Events</div></div>	<input type="radio"/> Not installed
	SlashNextSecurityEventsforMicrosoftSentinel	<input type="radio"/> Not installed
<input checked="" type="checkbox"/>	<div><div>▼</div><div> Windows Security Events</div></div>	<input type="radio"/> Not installed

Fig 21


13 | Page


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

[Install](#)

[View details](#)

Fig 22














<input type="checkbox"/>	▼  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.

- 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.**
- 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 ⓘ

Manage

Actions ▼

[View details](#)

Fig 24

<input type="checkbox"/>	Content name		Created content	Conte...	Version	Status
<input type="checkbox"/>	Security Events via Legacy Agent		1 items	Data co...	1.0.0	Install
<input checked="" type="checkbox"/>	Windows Security Events via AMA		1 items	Data co...	1.0.0	Install
<input type="checkbox"/>	AD FS Remote Auth Sync Connection		--	Analyti...	1.0.4	Install
<input type="checkbox"/>	AD FS Remote HTTP Network Connection		--	Analyti...	1.0.2	Install
<input type="checkbox"/>	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.

Refresh

Rule name	Created by	Filter name
No results		

[+Create data collection rule](#)

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 \*

Subscription \* ⓘ

Resource group \* ⓘ

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.

**i** 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

Selected: All

Resource Groups

Selected: All

Resource Types

Selected: All

Locations

Selected: All

Show Selected

Fig 28

Ensure All security radio is checked.

### Create Data Collection Rule

Data collection rule management

Basic Resources Collect Review + create

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

Basic Resources Collect Review + create

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.

18 | Page

Extensions

VM Applications

+ Add

↻ Refresh

↑ Update

✓ Enable automatic upgrade

⏸ Disable automatic upgrade

🗉 Feedback

🔍 Search to filter items...

Showing all 1 items

<input type="radio"/>	Name	Type	Version	Latest Version	Status
<input type="radio"/>	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

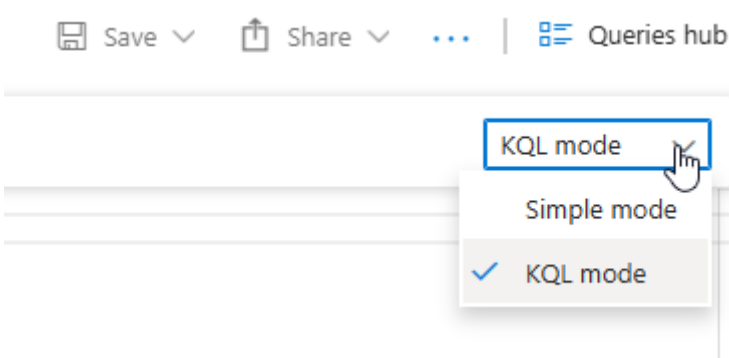


Fig 32

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

New Query 1*		Time range: Last 24 hours	Show: 5000 results
<pre>1 SecurityEvent 2   where EventID == 4625</pre>			
Results		Chart	
TimeGenerated [UTC]	Account	AccountType	Computer
9/6/2025, 10:46:50.690 AM	DESKTOP-ON6AJE5\demoUser1	User	HyperV-vm
9/6/2025, 10:46:21.882 AM	DESKTOP-ON6AJE5\Administra...	User	HyperV-vm
9/6/2025, 10:45:43.507 AM	DESKTOP-ON6AJE5\adminin	User	HyperV-vm
9/6/2025, 10:45:33.396 AM	DESKTOP-ON6AJE5\admin	User	HyperV-vm

Fig 33

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

Run

Time range : Last 24 hours

Show : 5000 results

```

1 SecurityEvent
2 | where EventID == 4625
3 | where Account == "\\KANTIN"
4 | project TimeGenerated, IPAddress
5
6
7
8
9
10

```

Results Chart

TimeGenerated [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

General

Source

Review + create

Name \*

Description

Alias \*

geoip

Map IP Address

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

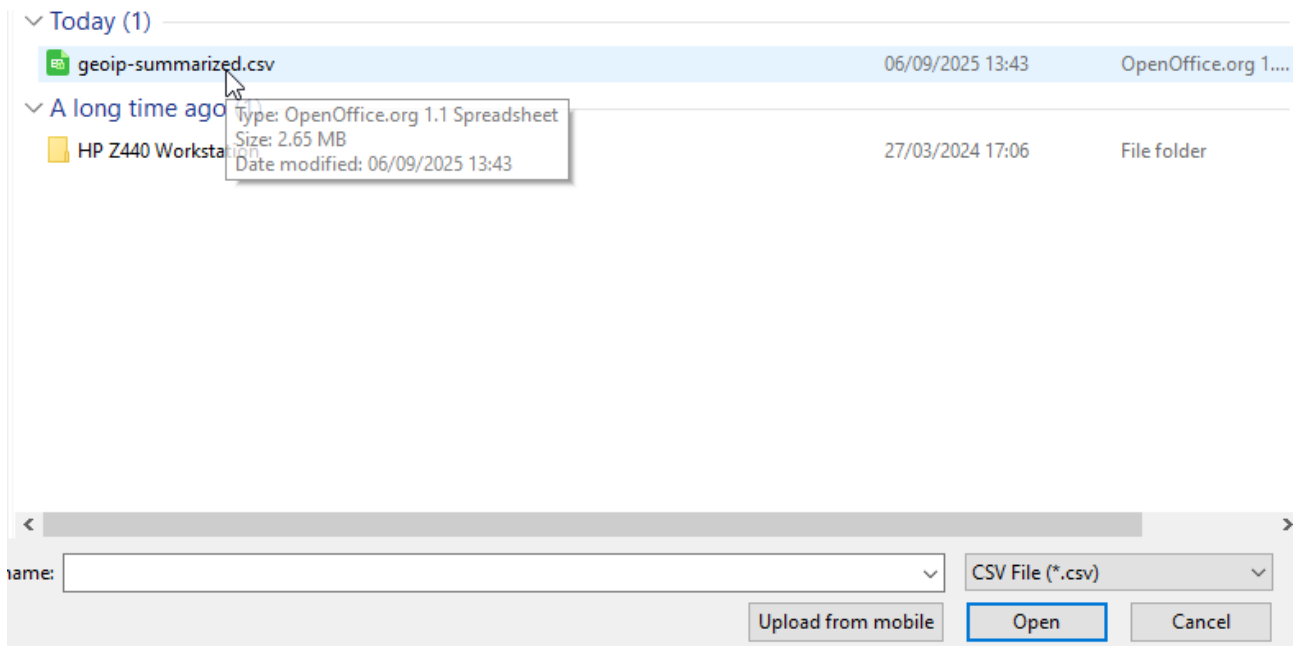


Fig 36

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

Drag and drop the files or  
Browse for files

SearchKey \* network


Reset




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


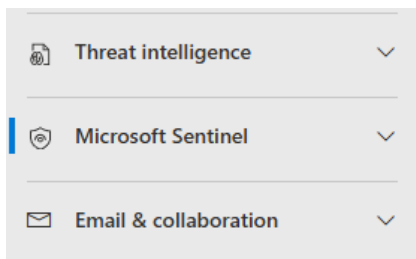
Status (Preview)  
 Succeeded

Fig 39



My workbooks Templates

+ Add Workbook

Search

Add filter

Favorite Name

Fig 40

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

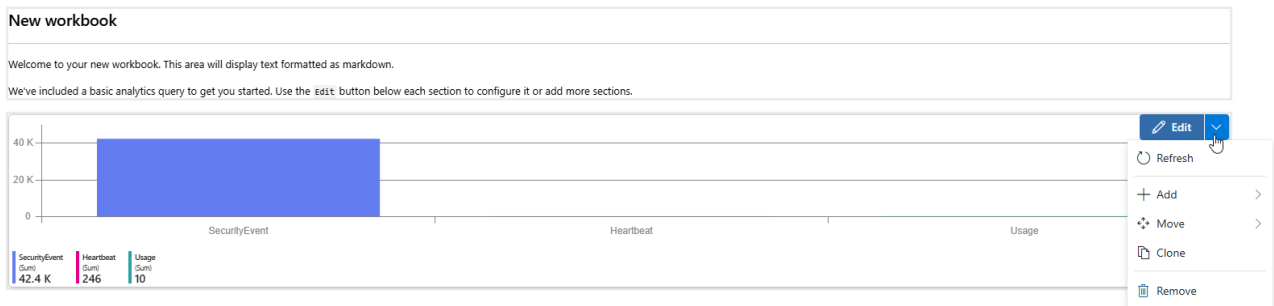


Fig 41

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

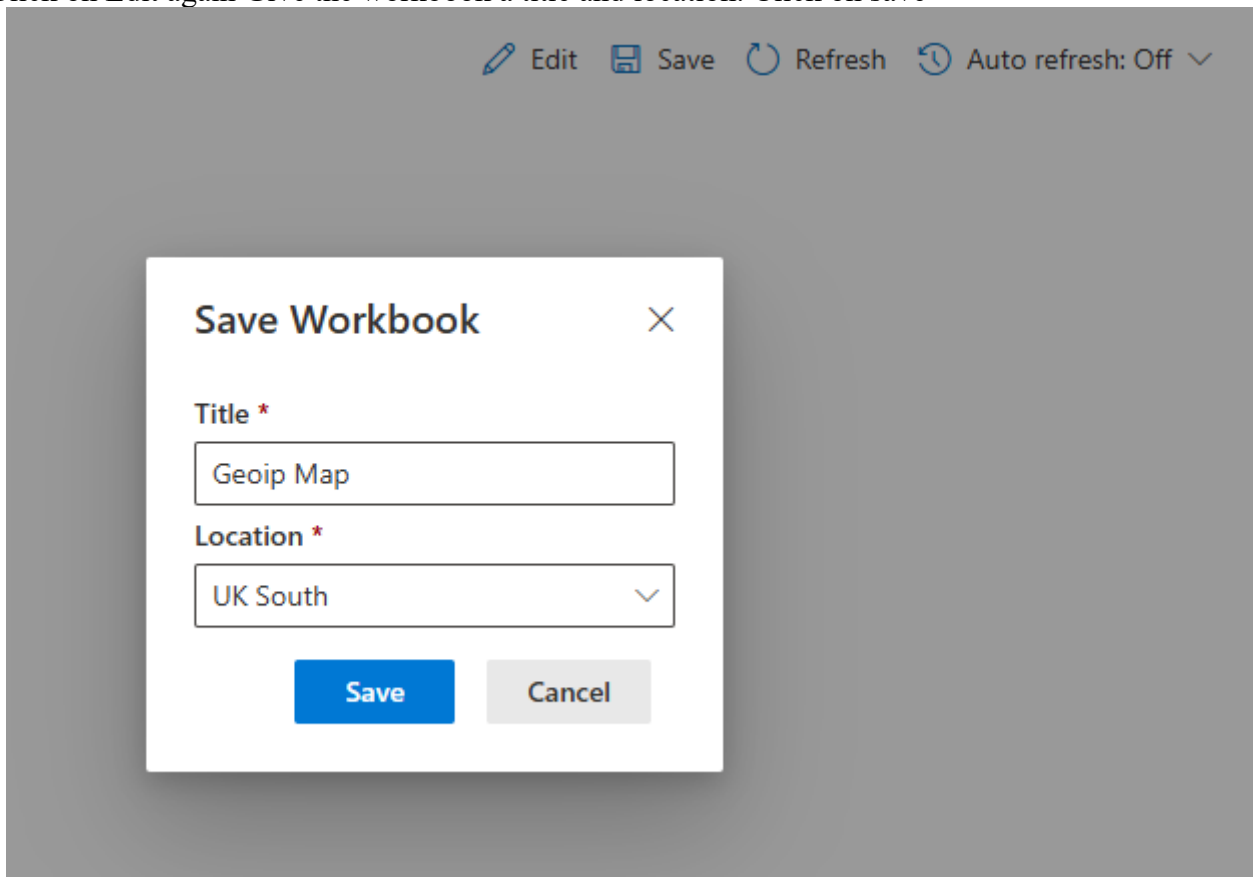


Fig 42

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](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.

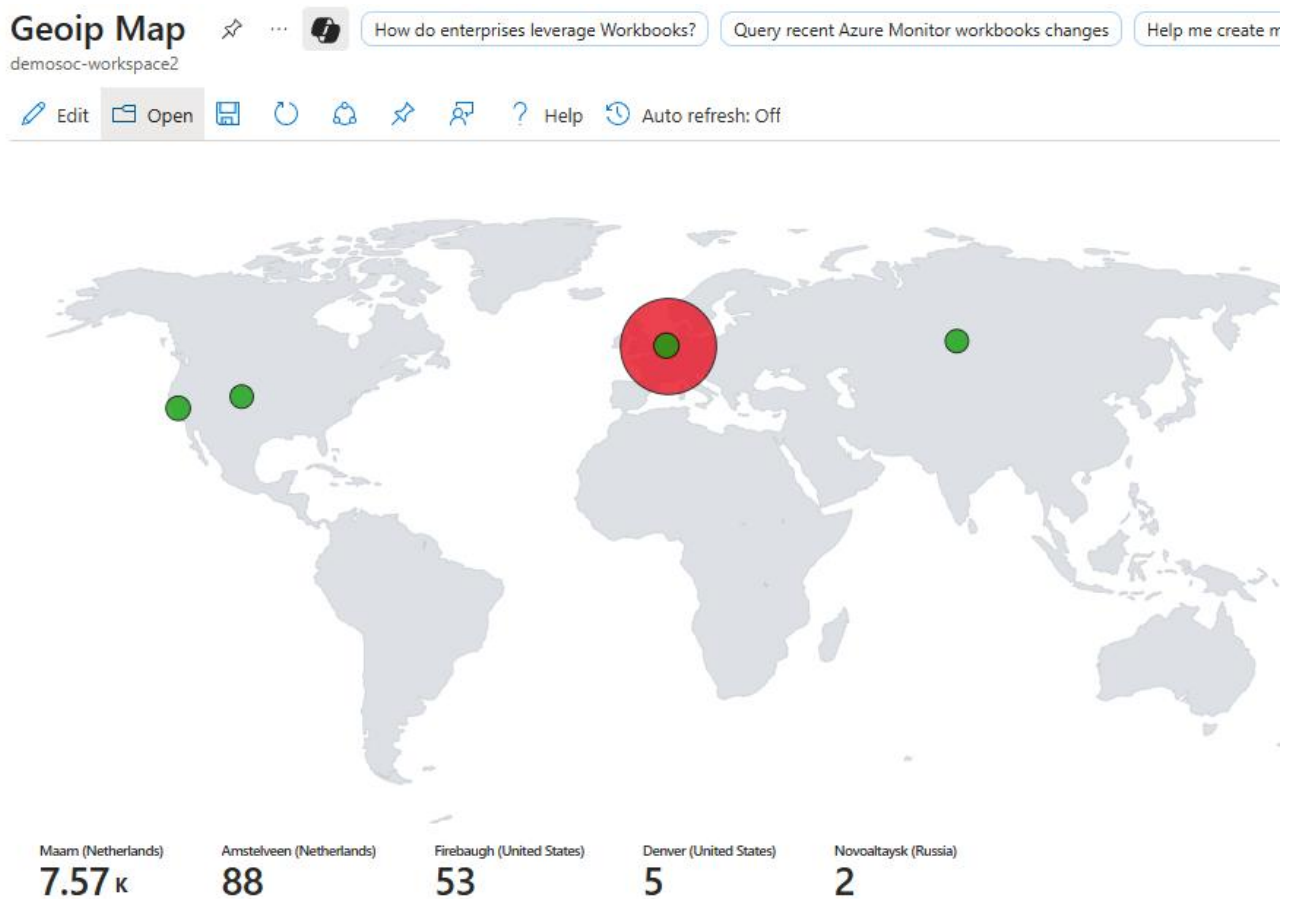


Fig 43

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.

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

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

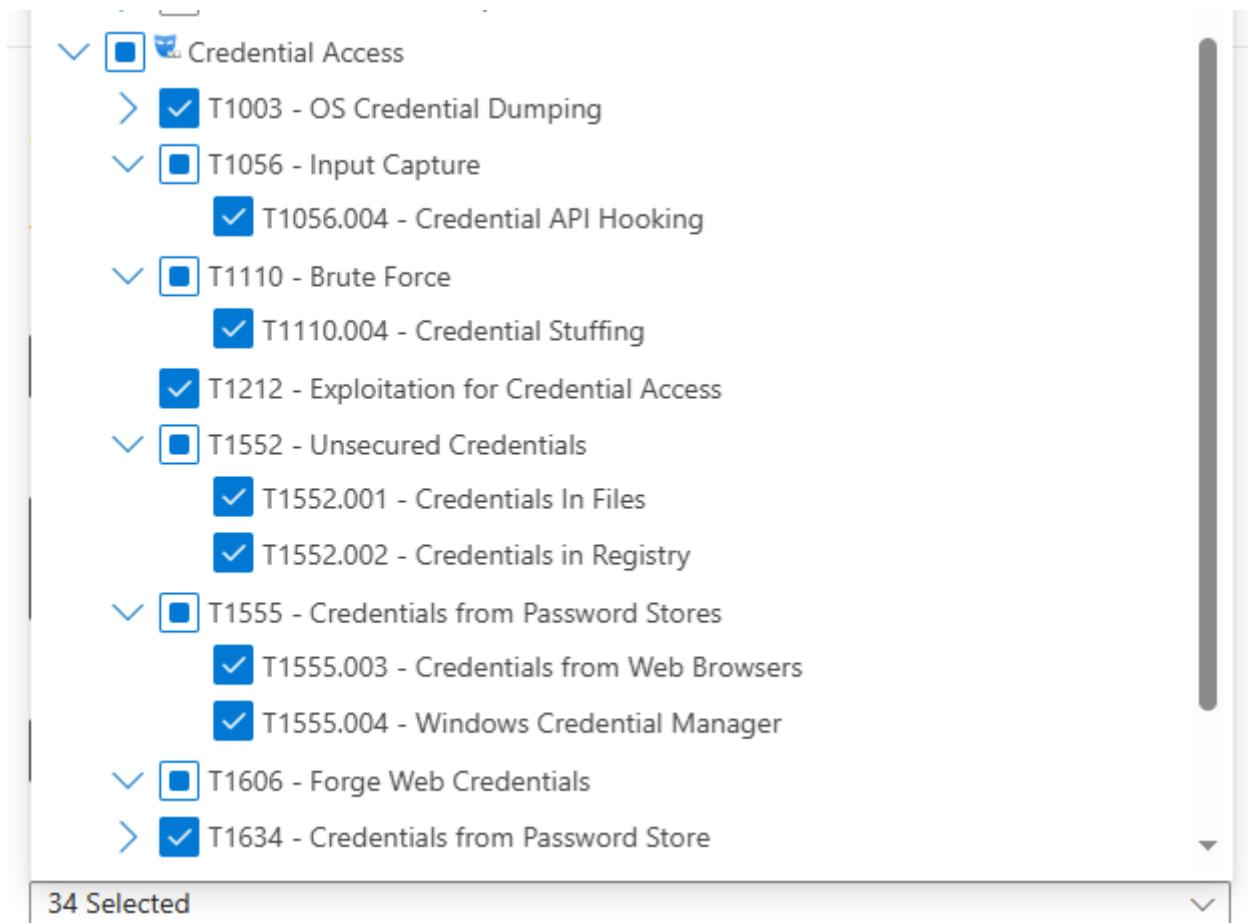


Fig 46

Set how often the rule will run.

### 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

① 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

① 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 \*

#### 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

↓ 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.

## 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@msokey69yahoomcom.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 execution 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 X

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

### Choose case to link to

Link

+ Create

1 selected

Customize columns

Last updated

Search

Filters:

Priority: Any

Status: Any

Assigned to: Any

Due on: Any

Created by: Any

Created on: Any

Add filter

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

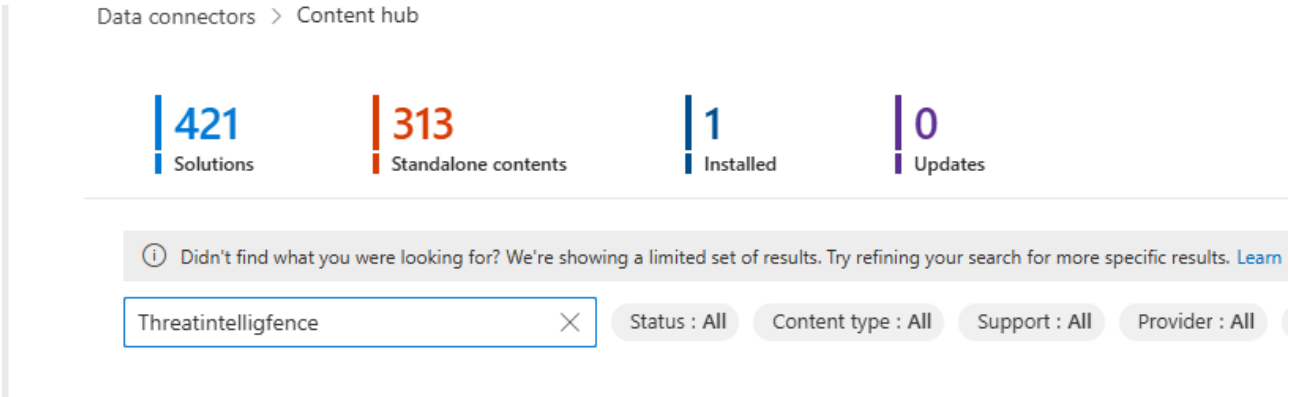


Fig 57

Select the first instance of Threat Intelligence

Install/Update

Delete

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

Install



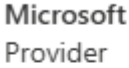


[View details](#) 

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

---

[Manage](#) [Actions](#) [View details](#)

Fig 60

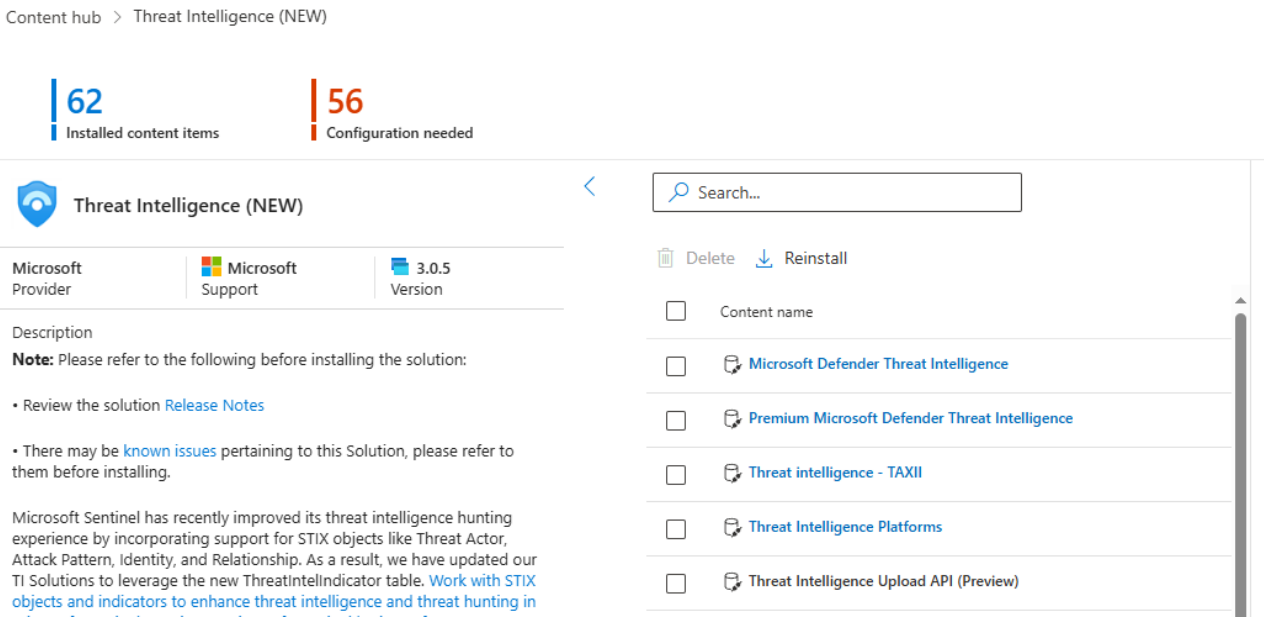


Fig 61

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

To receive data from Pulsedive and account is required.

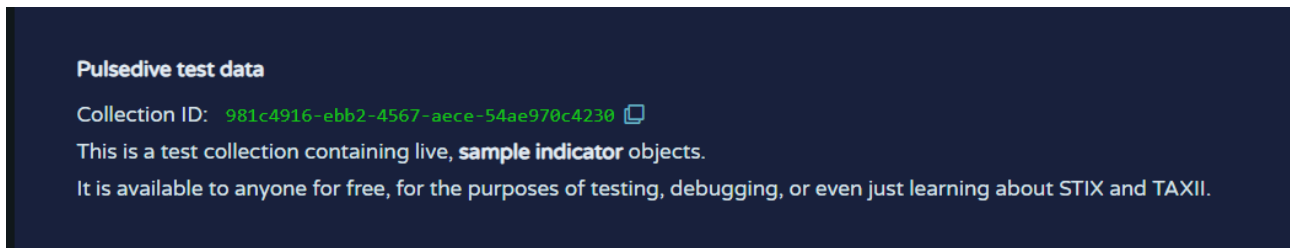


Fig 63

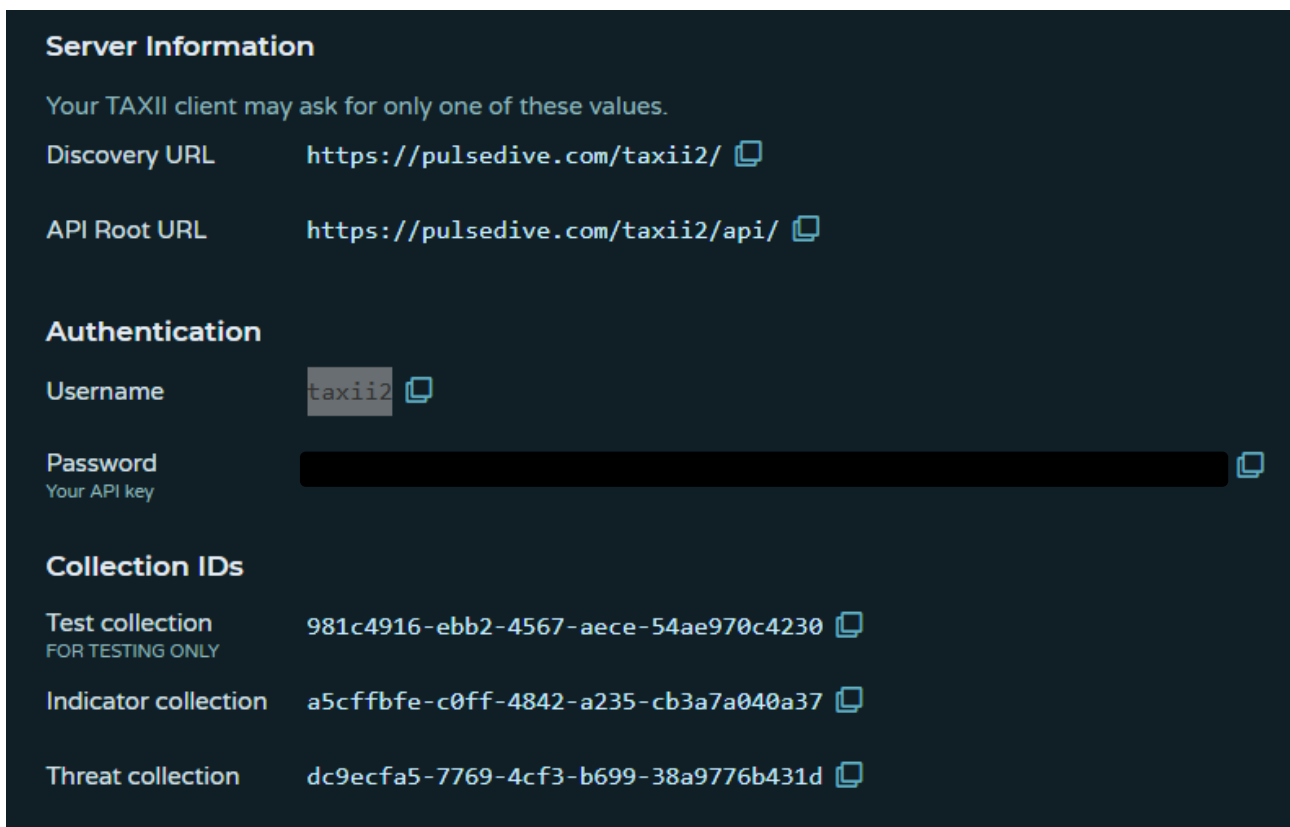


Fig 64

On the Threat intelligence page, click on Open connector page

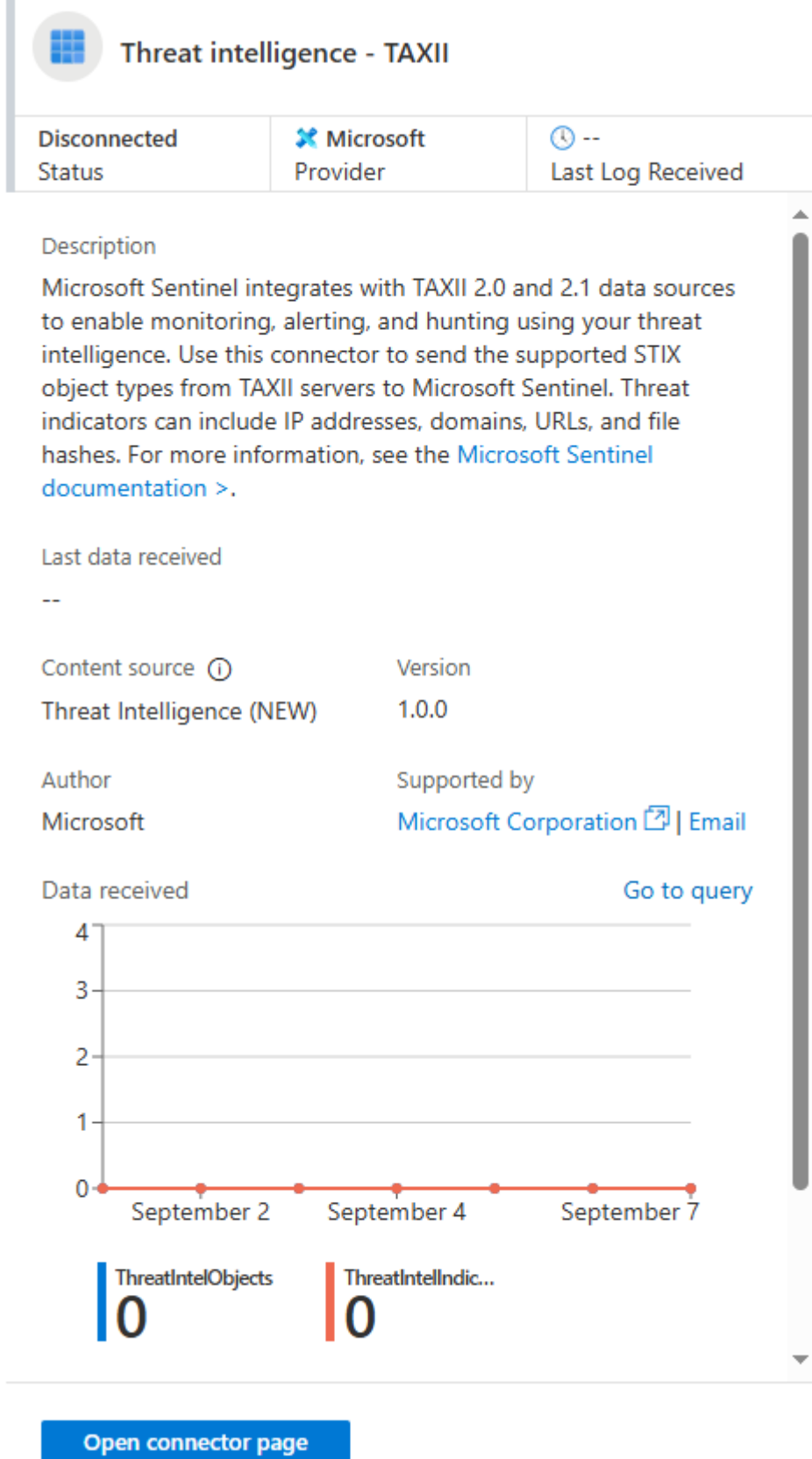


Fig 62



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

## 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 connect

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



**Add**

Fig 65

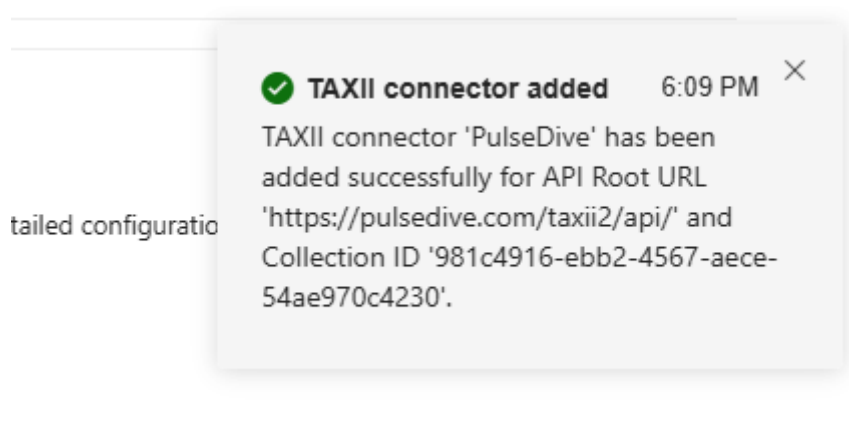





Fig 66



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 

Version


Threat Intelligence (NEW)

1.0.0

Author

Supported by

Microsoft

[Microsoft Corporation](#)  | [Email](#)

Related content

0

Workbooks

2

Queries

47

Analytics rules templates

Fig 67

42 | Page

Indicators (88,948)							
Attack patterns (0)							
Identities (1)							
Threat actors (0)							
Relationships (0)							
+ New <span>▼</span> <span>🔗 Add tags</span> <span>🗑 Delete</span> <span>📄 Columns</span>							
<input type="checkbox"/>	Values	Name	Types	Source	Confidence	Alerts	Tags
<input type="checkbox"/>	89.108.74.206	Detection Pattern	↔ IPv4 address	PulseDive	--	0	--
<input type="checkbox"/>	88.218.76.108	Detection Pattern	↔ IPv4 address	PulseDive	--	0	--
<input type="checkbox"/>	88.166.135.112	Detection Pattern	↔ IPv4 address	PulseDive	--	0	--
<input type="checkbox"/>	86.98.152.111	Detection Pattern	↔ IPv4 address	PulseDive	--	0	--
<input type="checkbox"/>	85.9.108.9	Detection Pattern	↔ IPv4 address	PulseDive	--	0	--
<input type="checkbox"/>	hls.tazieh.ir	Detection Pattern	🌐 Domain name	PulseDive	--	0	--
<input checked="" type="checkbox"/>	dl.tazieh.ir	Detection Pattern	🌐 Domain name	PulseDive	--	0	--
<input type="checkbox"/>	back.tazieh.ir	Detection Pattern	🌐 Domain name	PulseDive	--	0	--
<input type="checkbox"/>	87.237.226.247	Detection Pattern	↔ IPv4 address	PulseDive	--	0	--
<input type="checkbox"/>	87.225.40.249	Detection Pattern	↔ IPv4 address	PulseDive	--	0	--
<input type="checkbox"/>	87.205.110.7	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 metadata have been moved to the Content Hub.

ⓘ Device specific AMA connectors have been deprecated. [Learn more >](#)


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


8

Connectors

5

Connected

 More content at  
Content Hub

 Search by name or provider

Providers : All

Data Types : .









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

Fig 69

Indicators (88,998)    Attack patterns (0)    Identities (1)    Threat actors (0)    Relationships (0)							
+ New    Add tags    Delete    Columns							
<input type="checkbox"/> Values	Name	Types	Source	Confidence	Alerts	Tags	
<input type="checkbox"/> 185.243.96.105	Microsoft Identified IOC	Network traffic	Microsoft Defender Threat...	100	0	honeypot	
<input type="checkbox"/> 103.250.189.28	Microsoft Identified IOC	Network traffic	Microsoft Defender Threat...	100	0	honeypot	
<input type="checkbox"/> 100.42.180.31	Microsoft Identified IOC	Network traffic	Microsoft Defender Threat...	100	0	honeypot	
<input checked="" type="checkbox"/> 104.152.52.60	Microsoft Identified IOC	Network traffic	Microsoft Defender Threat...	100	0	honeypot	
<input type="checkbox"/> 51.83.96.232	Microsoft Identified IOC	Network traffic	Microsoft Defender Threat...	100	0	honeypot	
<input type="checkbox"/> 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    ic100    vic100    +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

- 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.
- 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.
- 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.
- Incident Handling Workflow:** The manual creation and assignment of incidents reinforced the structured workflow SOC analysts follow, from detection to investigation and resolution.
- 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.

