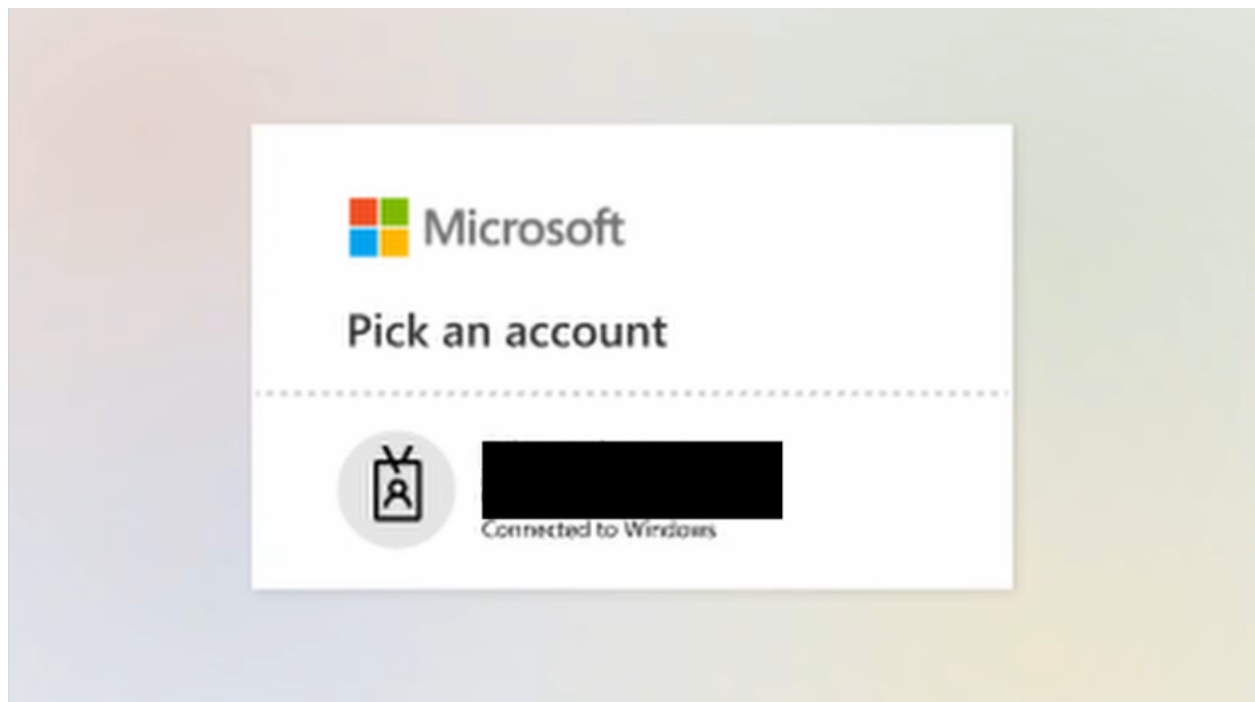


Installation Guide

For this project, we decided to use the cloud-based solution, Azure, created by Microsoft. We will explain the installation of our project and any maintenance needed for the future.

1. First, we make a Microsoft Azure account. FIU students should have access to their own Azure account with Office 365, simply login using your credentials. As a student you get a noticeable amount of credit to start off with. If not, you can simply use a standard Microsoft account, from that point on you will have to make your own Azure subscription. You can try Azure for free for 30 days, so make sure to take advantage of this.



- Next, we need to create a resource group. This will be the container that holds all related sources of your project such as the Virtual Machine, Log Analytics, etc.

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](#)

Project details

Subscription * ⓘ Visual Studio Enterprise Subscription

Resource group * ⓘ myResourceGroup0816 ✓

Resource details

Region * ⓘ (US) Central US

Review + create < Previous Next : Tags >

- Then, we will create a Virtual Machine, for this project we used Windows 10. Make sure to pay attention to the monthly cost.

Microsoft Azure Upgrade Search resources, services, and docs (G+/I) Copilot whitehatmat3@hotmail... DEFAULT DIRECTORY (WHITEHA...

Home > Compute infrastructure | Virtual machines >

Create a virtual machine

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my workload

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my workload

Availability zone * ⓘ Zone 2

You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#)

Security type ⓘ Standard

Image * ⓘ Windows 10 Enterprise LTSC 2021 - x64 Gen1 (free services eligible)

[See all images](#) | [Configure VM generation](#)

There is a generation 2 version of this image available which has higher feature compatibility. [Click here to swap to the generation 2 version](#)

VM architecture ⓘ

☐ Arm64

☒ x64

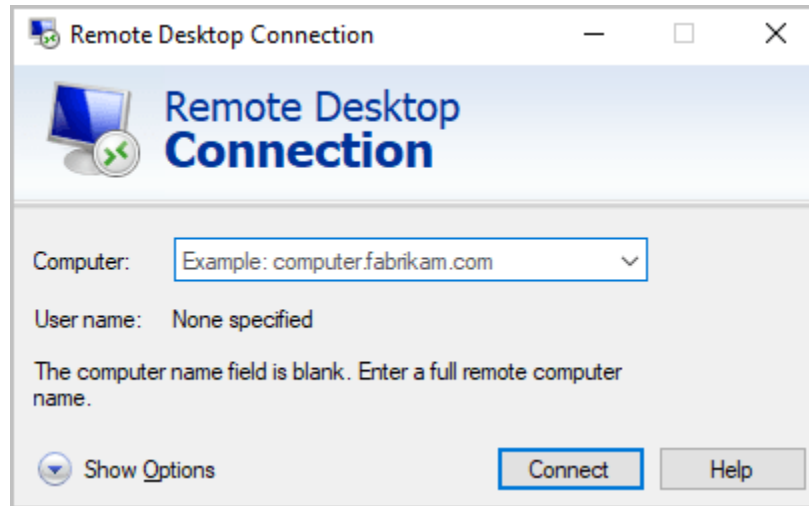
Arm64 is not supported with the selected image.

Run with Azure Spot discount ⓘ ☐

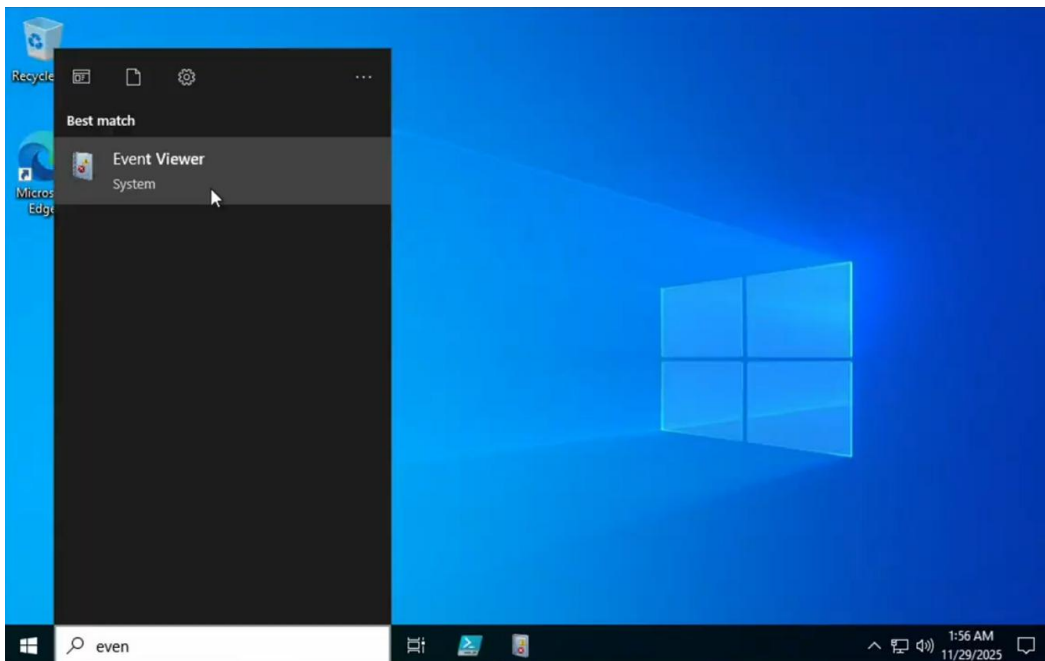
You are in the free trial period. Costs associated with this VM can be covered by any remaining credits on your subscription. [Learn more](#)

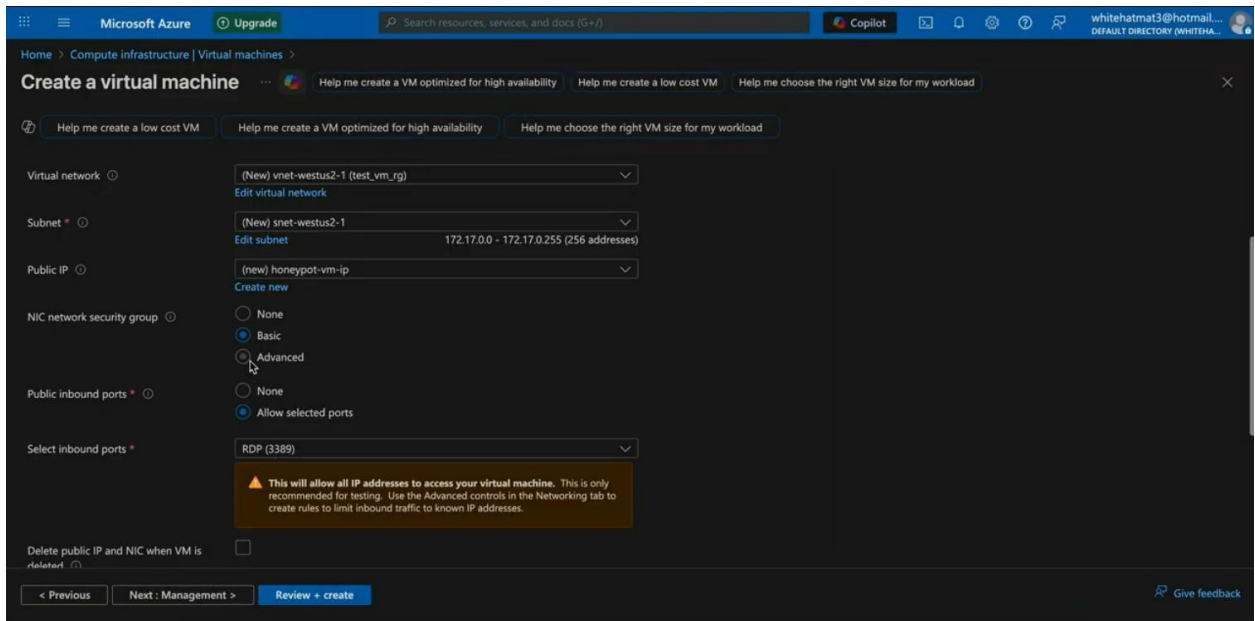
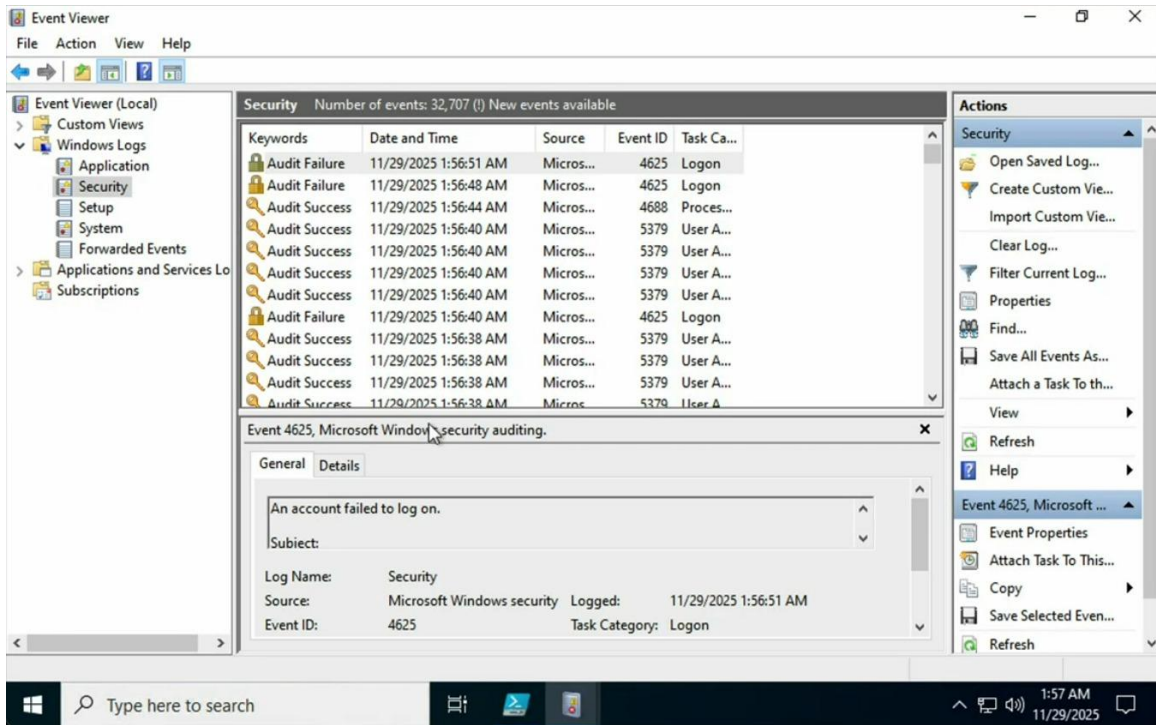
< Previous Next : Disks > Review + create Give feedback

4. Once it is booted, use Remote Desktop Connection to login, you can test that you are receiving logs through there with Event Viewer.



5. **NOTE: We want to focus on event ID 4625, which is the failed login event.**
Afterwards, create a virtual network and make it as open as possible. The intention is to create a honeypot to allow anyone to potentially interact with the machine.





Microsoft Azure

Upgrade

Search resources, services, and docs (G+7)

Copilot

whitehatmat3@hotmail...
DEFAULT DIRECTORY (WHITEHA...

Home > Compute infrastructure > Virtual machines >

Create network security group ...

Name *

honeypot-vm-nsg

Inbound rules ⓘ

No results.

+ Add an inbound rule

Outbound rules ⓘ

No results.

+ Add an outbound rule

OK

Add inbound security rule

honeypot-vm-nsg

X

Source ⓘ

Any

Source port ranges ⓘ

*

Destination ⓘ

Any

Service ⓘ

Custom

Destination port ranges * ⓘ

8080

Protocol

☒ Any

☐ TCP

☐ UDP

☐ ICMPv4

☐ ICMPv6

Action

☒ Allow

☐ Deny

Add

Cancel

Give feedback

Microsoft Azure

Upgrade

Search resources, services, and docs (G+7)

Copilot

whitehatmat3@hotmail...
DEFAULT DIRECTORY (WHITEHA...

Home > Compute infrastructure > Virtual machines >

Create network security group ...

Name *

honeypot-vm-nsg

Inbound rules ⓘ

No results.

+ Add an inbound rule

Outbound rules ⓘ

No results.

+ Add an outbound rule

OK

Add inbound security rule

honeypot-vm-nsg

X

Destination port ranges * ⓘ

*

Protocol

☒ Any

☐ TCP

☐ UDP

☐ ICMPv4

☐ ICMPv6

Action

☒ Allow

☐ Deny

Priority * ⓘ

100

Name *

inbound_insecu

Description

Add

Cancel

Give feedback

- Next we are going to create a Log Analytics Workspace. Once created, create an instance of Sentinel and connect it to our workspace.

The screenshot shows the 'Create Log Analytics workspace' wizard in the Microsoft Azure portal. The page has a dark theme. At the top, there's a navigation bar with 'Microsoft Azure' and an 'Upgrade' button. Below the navigation bar, the breadcrumb is 'Home > Log Analytics workspaces >'. The main heading is 'Create Log Analytics workspace'. A blue information box states: '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](#)'. Below this, a paragraph explains: '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.' The 'Project details' section asks to 'Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.' It has two dropdowns: 'Subscription' (set to 'Azure subscription 1') and 'Resource group' (set to 'test_vm_rg' with a 'Create new' link below it). The 'Instance details' section has two dropdowns: 'Name' (set to 'law-test-vm') and 'Region' (set to 'West US 2'). At the bottom, there are three buttons: 'Review + Create' (highlighted in blue), '< Previous', and 'Next: Tags >'.

The screenshot shows the 'Add Microsoft Sentinel to a workspace' wizard in the Microsoft Azure portal. The page has a dark theme. At the top, there's a navigation bar with 'Microsoft Azure' and an 'Upgrade' button. Below the navigation bar, the breadcrumb is 'Home > Microsoft Sentinel >'. The main heading is 'Add Microsoft Sentinel to a workspace'. There are two buttons: '+ Create a new workspace' and 'Refresh'. A purple banner states: 'Microsoft Sentinel offers a 31-day free trial. See [Microsoft Sentinel pricing](#) for more details.' Below this, a blue information box states: 'New Microsoft Sentinel workspaces created by authorized users are automatically onboarded and redirected to the Defender portal. [Learn more](#)'. There's a search bar 'Filter by name...'. Below it is a table with the following columns: 'Workspace', 'Location', 'ResourceGroup', 'Subscription', and 'Directory'. The table has one row with the following data: 'test-vm', 'westus2', 'test_vm_rg', 'Azure subscription 1', and 'Default Directory'. At the bottom, there are two buttons: 'Add' (highlighted in blue) and 'Cancel'.

Workspace	Location	ResourceGroup	Subscription	Directory
test-vm	westus2	test_vm_rg	Azure subscription 1	Default Directory

7. From Sentinel, navigate to content hub and Windows Security Events, install it, then hit manage when done. Once there install “Windows Security Events via AMA”.

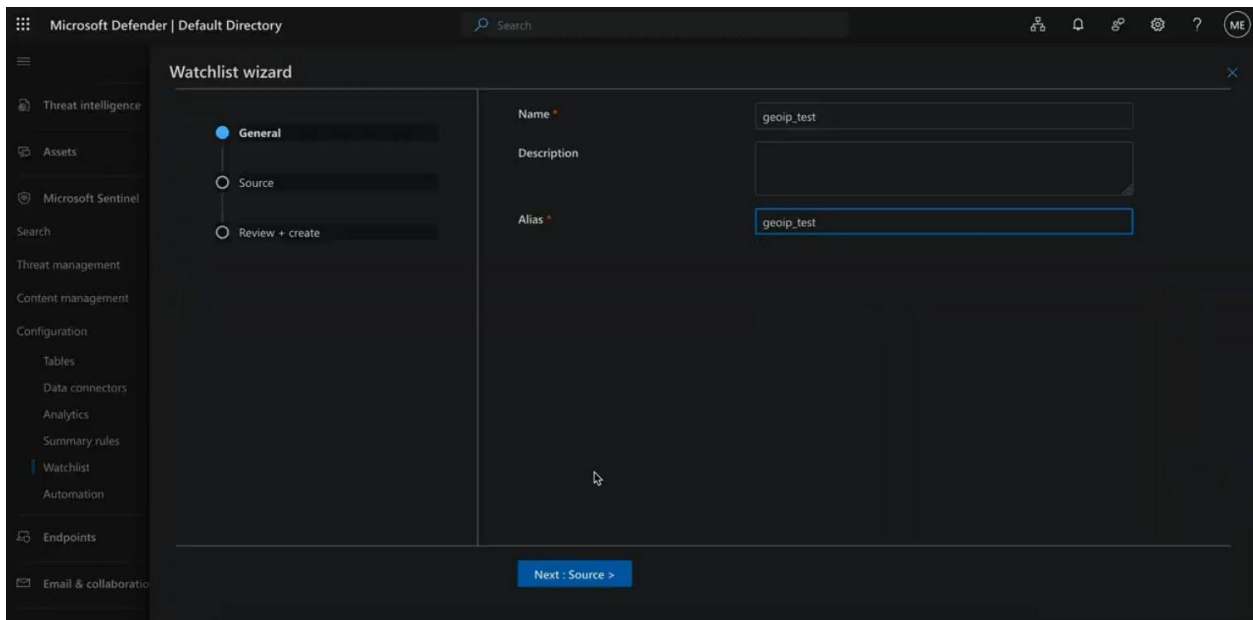
The screenshot shows the Microsoft Defender Content Hub interface. The left sidebar contains navigation options: Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Search, Threat management, Content management, Content hub (selected), Repositories, Community, Configuration, and Endpoints. The main area displays search results for 'windows security'. At the top, there are statistics: 448 Solutions, 317 Standalone contents, 0 Installed, and 0 Updates. A search bar shows 'windows security' with a filter icon. Below the search bar, there are tabs for Status (All), Content type (All), Support (All), Provider (All), Category (All), and Content source (All). A table lists the search results, showing columns for Content title, Status, and Content source. The first result is 'Windows Security Events' with a status of 'Not installed'. The second result is 'Windows Security Events via AMA' with a status of 'Not installed'. The third result is 'Security Events via Legacy Agent' with a status of 'Not installed'. The table is paginated, showing 'Page 1 of 2' and 'Showing 1 to 20 of 26 results'.

The screenshot shows the Microsoft Defender Content Hub interface with detailed information for the 'Security Events via Legacy Agent' solution. The left sidebar is the same as the previous screenshot. The main area displays the search results for 'Security Events via Legacy Agent'. The table shows the following results:

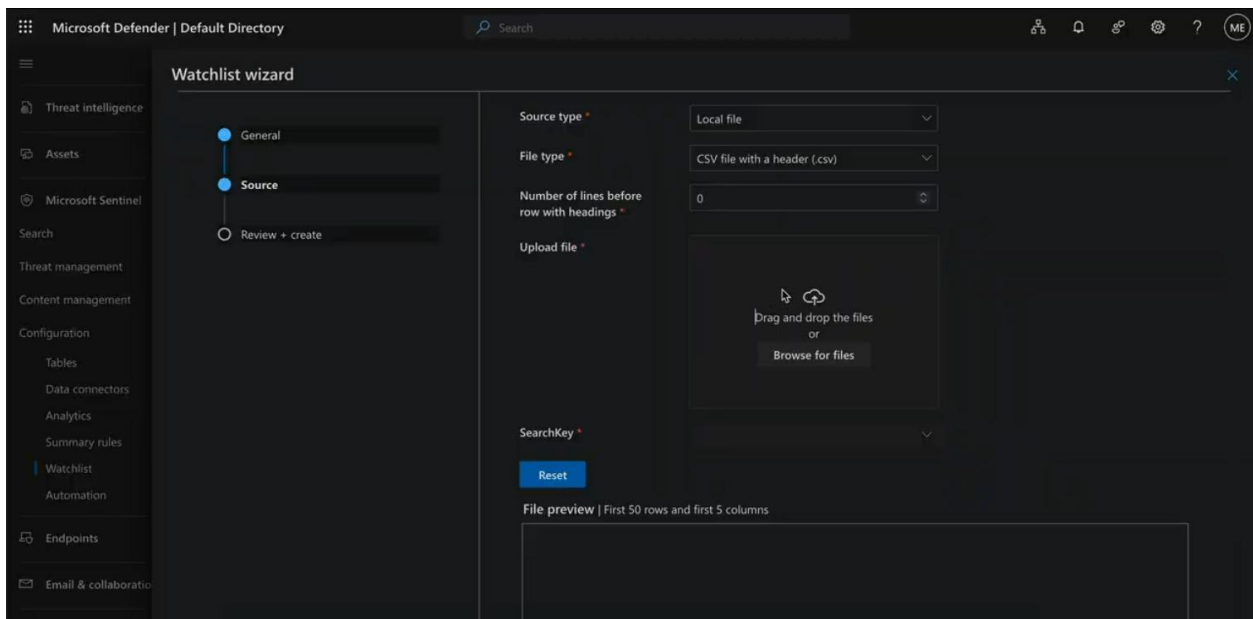
Content title	Status	Content source
Security Events via Legacy Agent	Not installed	Solu
NRT Security Event log cleared	Not installed	Solu
Windows System Time changed on hosts	Not installed	Solu
Suspicious Windows Login Outside Normal Ho...	Not installed	Solu
Excessive Windows Logon Failures	Not installed	Solu
Windows System Shutdown/Reboot(Systemon)	Not installed	Solu
NRT Base64 Encoded Windows Process Comm...	Not installed	Solu
New EXE deployed via Default Domain or Defa...	Not installed	Solu
Gain Code Execution on ADFS Server via SMB ...	Not installed	Solu
Starting or Stopping HealthService to Avoid De...	Not installed	Solu
Process Execution Frequency Anomaly	Not installed	Solu
AD FS Remote Auth Sync Connection	Not installed	Solu
Potential Fodhelper UAC Bypass	Not installed	Solu
AD user enabled and password not set within 4...	Not installed	Solu
Scheduled Task Hide	Not installed	Solu

The table is paginated, showing 'Page 1 of 2' and 'Showing 1 to 20 of 26 results'. On the right side, there is a detailed description of the 'Security Events via Legacy Agent' solution. It includes a note: '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.' Below the note, there are statistics: 'Data Connectors: 2, Workbooks: 2, Analytic Rules: 20, Hunting Queries: 50'. There are also links to 'Learn more about Microsoft Sentinel' and 'Learn more about Solutions'. At the bottom, there is an 'Install' button and a 'View details' link.

- Next we create a watchlist using an imported spreadsheet containing a vast number of IP addresses associated with a geographic location, containing latitude and longitude as well.



The screenshot shows the 'Watchlist wizard' in the Microsoft Defender interface. The left sidebar contains a navigation menu with options like Threat intelligence, Assets, Microsoft Sentinel, Search, Threat management, Content management, Configuration, Tables, Data connectors, Analytics, Summary rules, Watchlist (highlighted), Automation, Endpoints, and Email & collaboration. The main panel is titled 'Watchlist wizard' and has three steps: General (selected), Source, and Review + create. The 'General' step contains fields for Name (filled with 'geoip_test'), Description (empty), and Alias (filled with 'geoip_test'). A 'Next : Source >' button is at the bottom right.



The screenshot shows the 'Watchlist wizard' in the Microsoft Defender interface, now on the 'Source' step. The left sidebar is the same as the previous screenshot. The main panel has the 'Source' step selected. It contains fields for Source type (dropdown, 'Local file'), File type (dropdown, 'CSV file with a header (.csv)'), Number of lines before row with headings (input, '0'), and Upload file (a button). Below these is a 'SearchKey' dropdown and a 'Reset' button. At the bottom, there is a 'File preview' section with the text 'File preview | First 50 rows and first 5 columns' and an empty table area.

Microsoft Defender | Default Directory

Search

Watchlist wizard

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	17.8847	102.7384	Nong Khai	Thailand

9. Once created, we can observe the logs using KQL and see where the events are coming from.

New Query 1* ... x +

Save Share ... Queries hub

Run Time range: Last 24 hours Show: 1000 results KQL mode

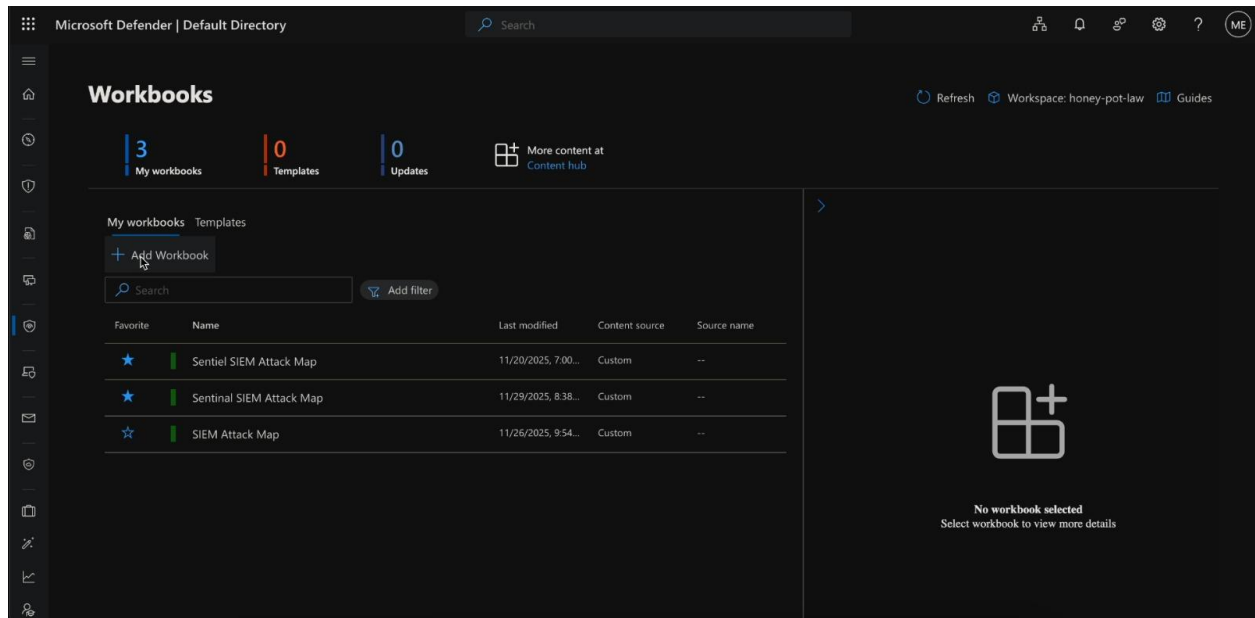
1 SecurityEvent

Results Chart

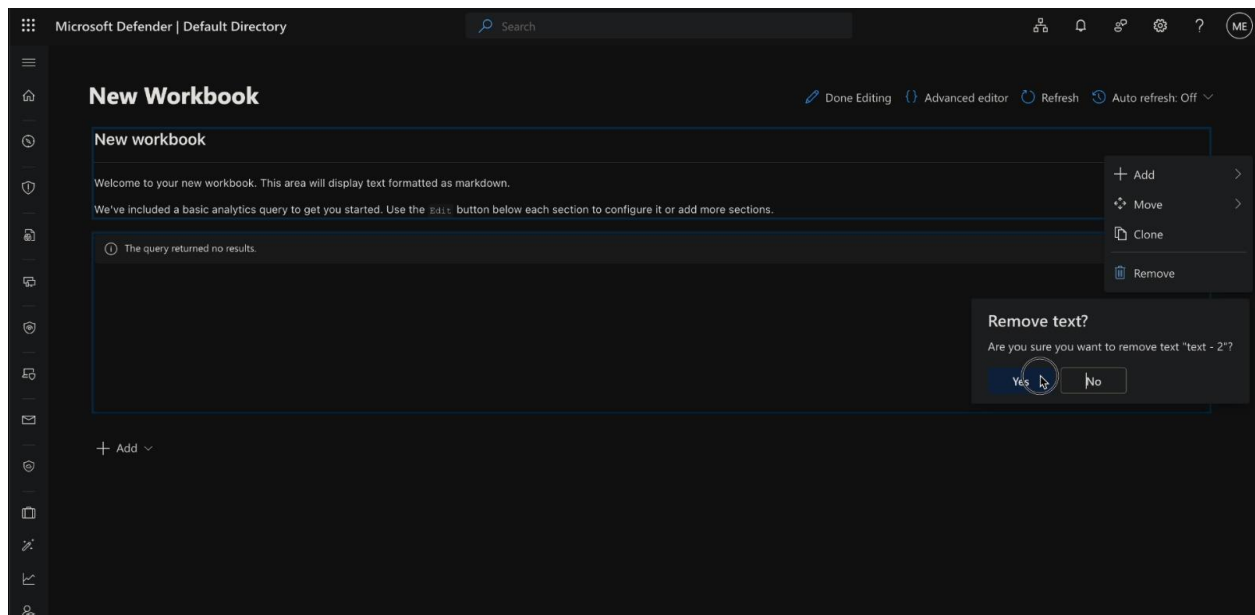
TimeGenerated [UTC] ↑↓	Account	AccountType	Computer	EventSourceName
> 11/29/2025, 2:43:47.089 AM	\ADMINISTRATOR	User	honey-pot-vm	Microsoft-Windows-Security-Auditing
> 11/29/2025, 2:43:45.373 AM	\USER	User	honey-pot-vm	Microsoft-Windows-Security-Auditing
> 11/29/2025, 2:43:43.192 AM	\ADMINISTRATOR	User	honey-pot-vm	Microsoft-Windows-Security-Auditing
> 11/29/2025, 2:43:37.136 AM	\ADMIN	User	honey-pot-vm	Microsoft-Windows-Security-Auditing
> 11/29/2025, 2:43:33.448 AM	\USER9	User	honey-pot-vm	Microsoft-Windows-Security-Auditing
> 11/29/2025, 2:43:29.015 AM	\ADMINISTRATOR	User	honey-pot-vm	Microsoft-Windows-Security-Auditing
> 11/29/2025, 2:43:24.042 AM	\ADMINISTRATOR	User	honey-pot-vm	Microsoft-Windows-Security-Auditing

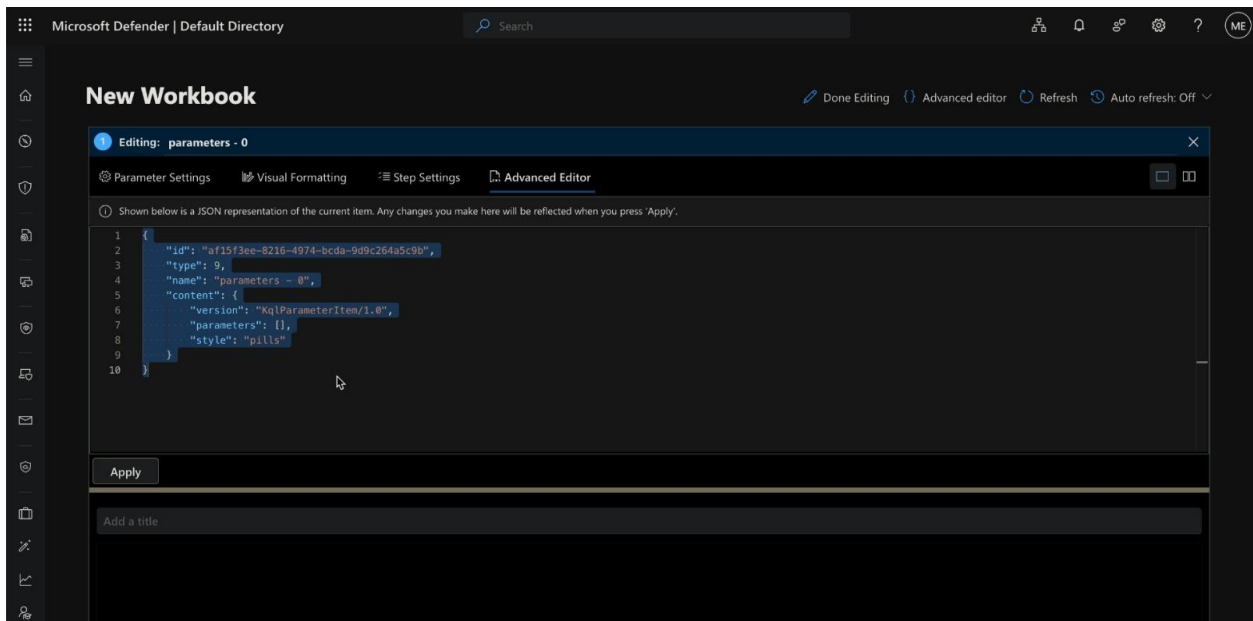
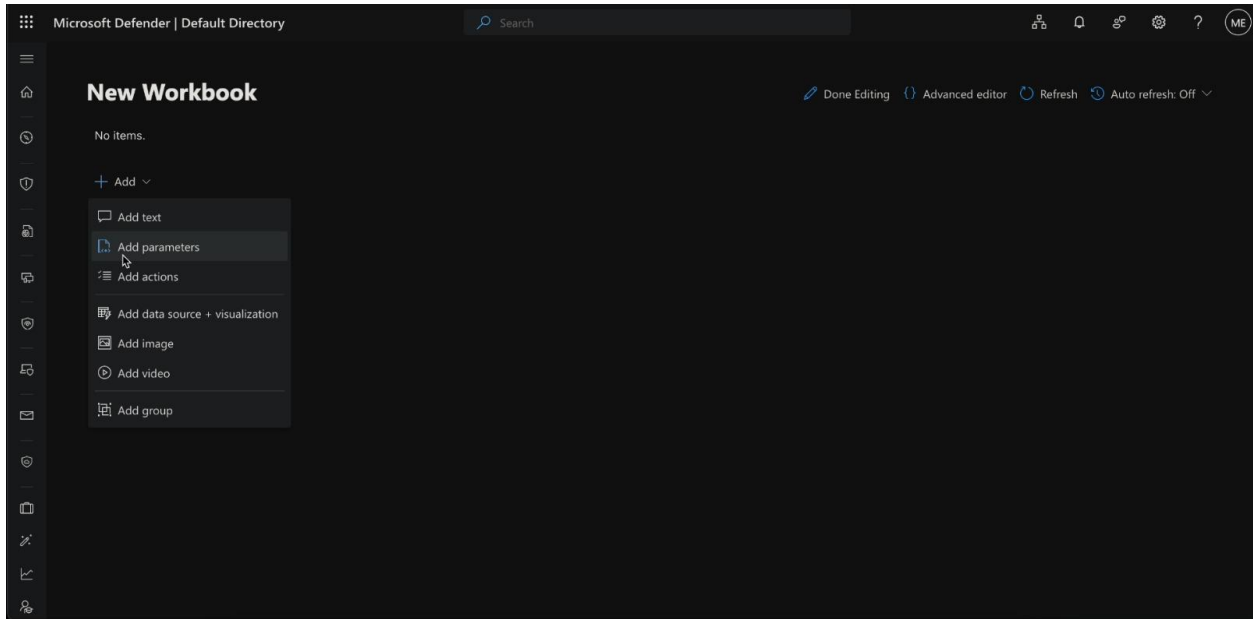
2s 603ms Display time (UTC+00:00) Query details 1 - 8 of 1000

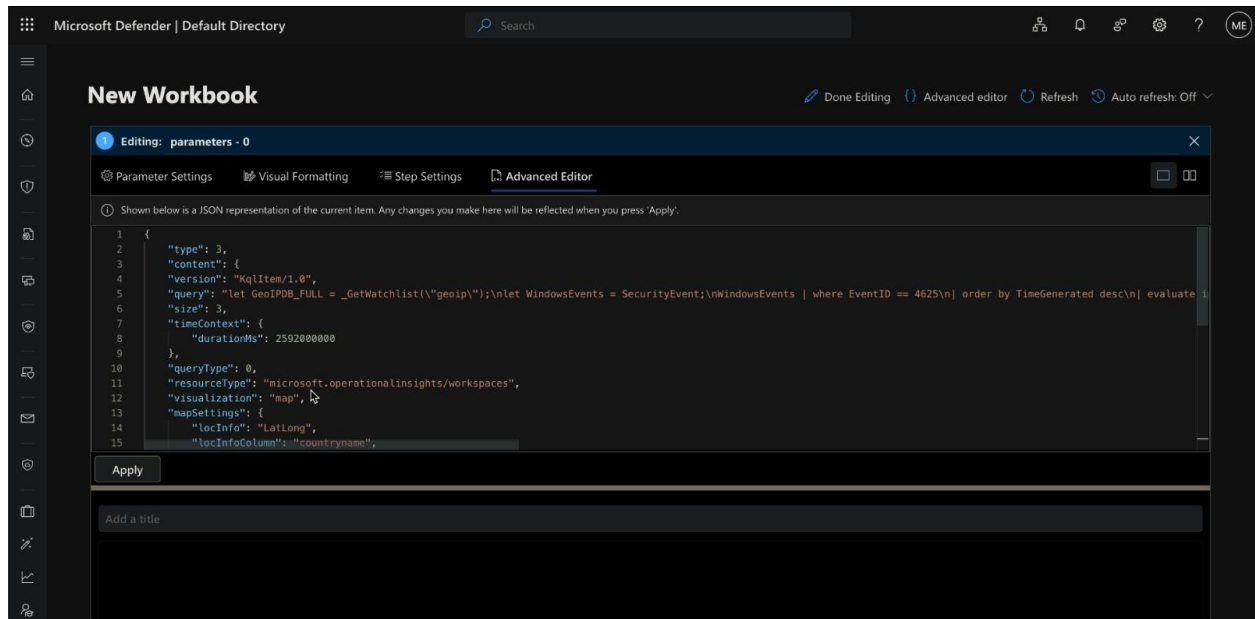
10. Finally, in Sentinel, create a new workbook.



11. From there, click edit and delete the existing elements shown in the workbook and replace it using the Query tab and paste in the JSON script with the map.







Good job, you are now ready to collect logs and see the locations of these failed login attempts from your very own attack map. The longer the VM is up, the more logs get collected, therefore the more your attack map begins to grow. Make sure to keep track of changes and pricing throughout your time when running this VM. You can check billing and spending trends on Azure in the billing section.