Map Cyber Attacks by Using Microsoft Sentinel

Challenge Overview

Understand the scenario

You are a new trainee for Hexelo, an organization that needs to train employees on how to use Microsoft Sentinel. First, you will create a new resource group, and then you will create a Log Analytics Workspace and add Microsoft Sentinel to the workspace. Next, you will create a new virtual machine, and then you will connected a workspace to a virtual machine by using Remote Desktop Connection. Finally, you will create a new workbook, and then you will visualize the attacks on a map.

Navigating the Challenge Lab

▼ Quick tips for navigating the Challenge Lab instructions.

Select the Copy to Clipboard icon to copy the green text.

Select the Type Text icon to insert the green text directly into the Challenge Lab environment.

An Alert tells you that a task requires extra care.

A Note provides additional helpful information for completing a task.

A Hint will guide you through a portion of the Challenge Lab.

A Knowledge block provides a deeper level of knowledge into a subject. It is a great way to solidify your understanding, but it is not strictly necessary to complete the Challenge Lab.

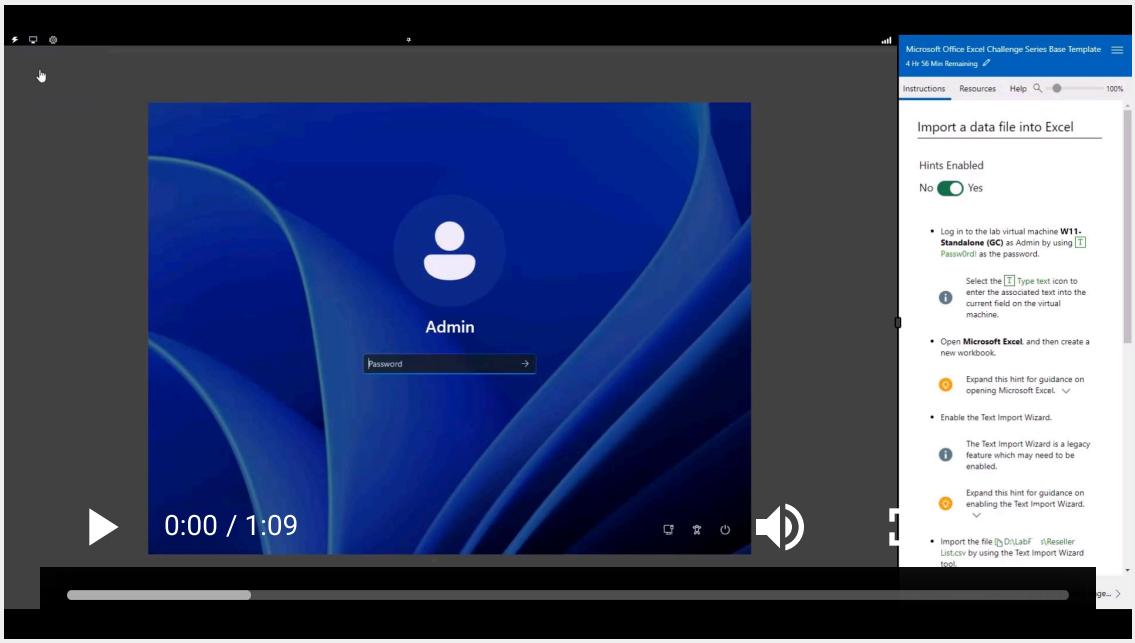
Add Microsoft Sentinel to a workspace

Hints Enabled

No Yes

- Sign in to **Windows 11** as T Administrator by using T Passw0rd! as the password.

Expand this hint for guidance on logging in to a Virtual Machine (VM):

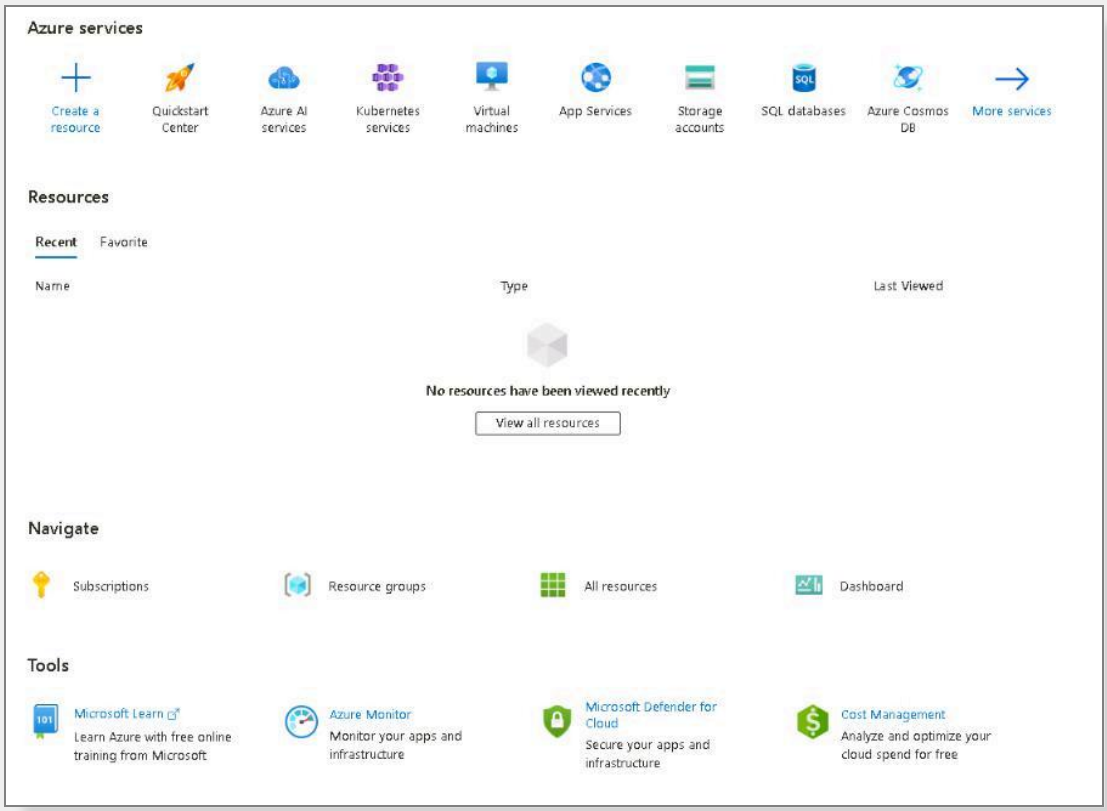


Select the T Type Text icon to enter the associated text into the virtual machine.

- Navigate to T https://portal.azure.com, and then sign-in as T {USERNAME} by using T {PASSWORD} as the password .

Expand this hint for guidance on signing into the Azure portal.

- Open a new browser tab, and then go to T https://portal.azure.com.
- Sign in as T {USERNAME} by using T {PASSWORD} as the password.
- If asked to save the password, select **Never**.
- If asked to Stay signed in, select **No**.
- Close any Welcome pages.

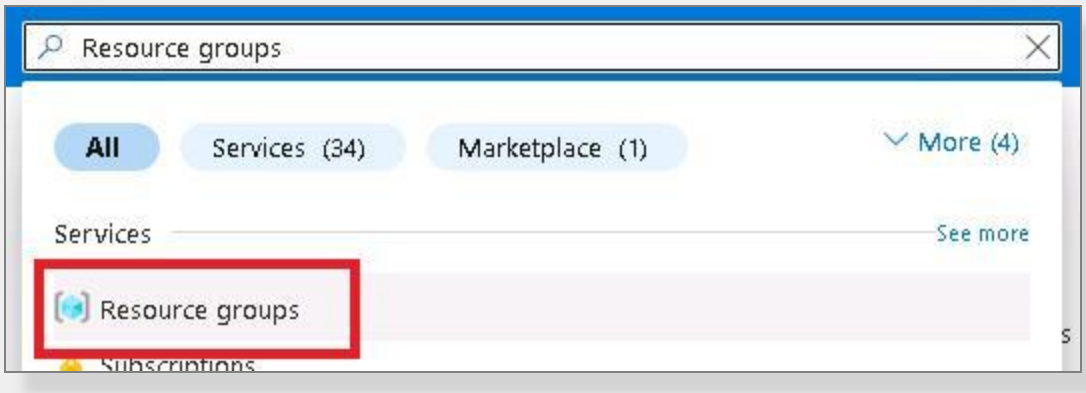


Want to learn more? Review the documentation on signing into the Azure portal.

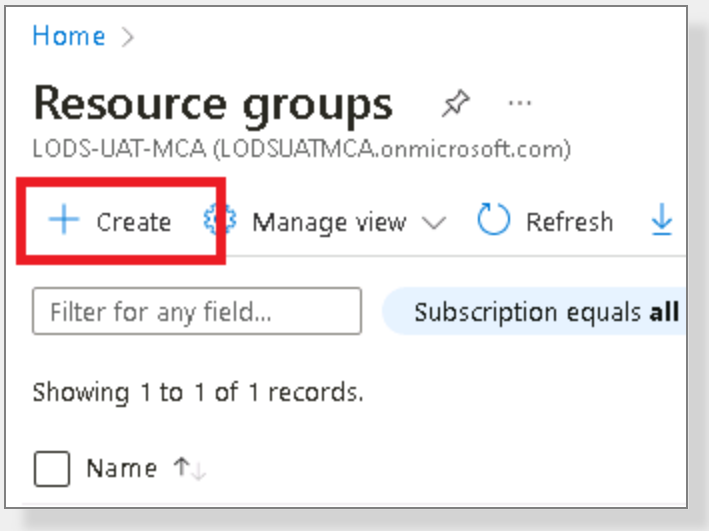
- Create a new Resource group named T SentinelHexelo-RG in the **East US region**.

Expand this hint for guidance on creating a Resource group.

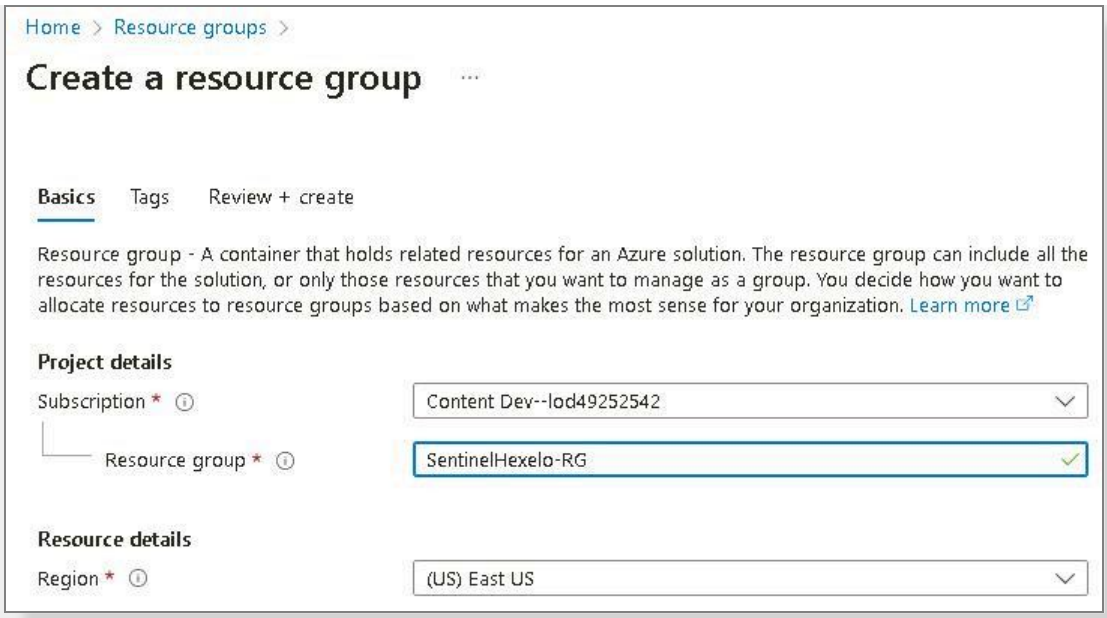
- On the Microsoft Azure home page, in Search resources, services, and docs (G+/), search for and select T Resource groups.



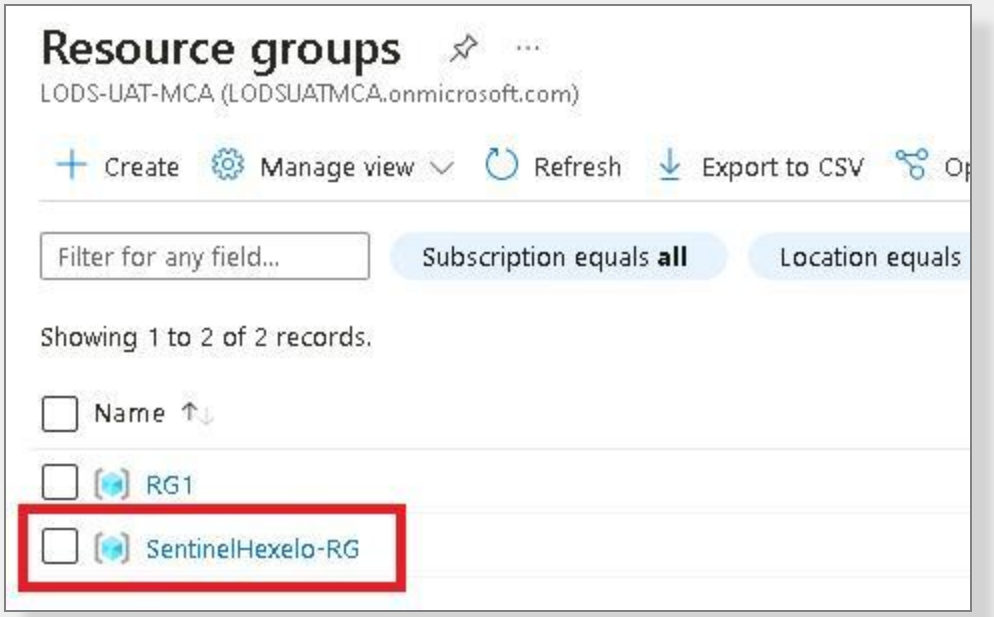
- On the Resource groups page, select **Create**.



- On the Create a resource group page, select your Subscription, and then in Resource group, enter T SentinelHexelo-RG.
- In Region, select East US, and then select **Review + Create**.



- On the Review + create tab, verify that the resource group has passed validation, and then select **Create**.



Want to learn more? Review the documentation on creating a resource group.

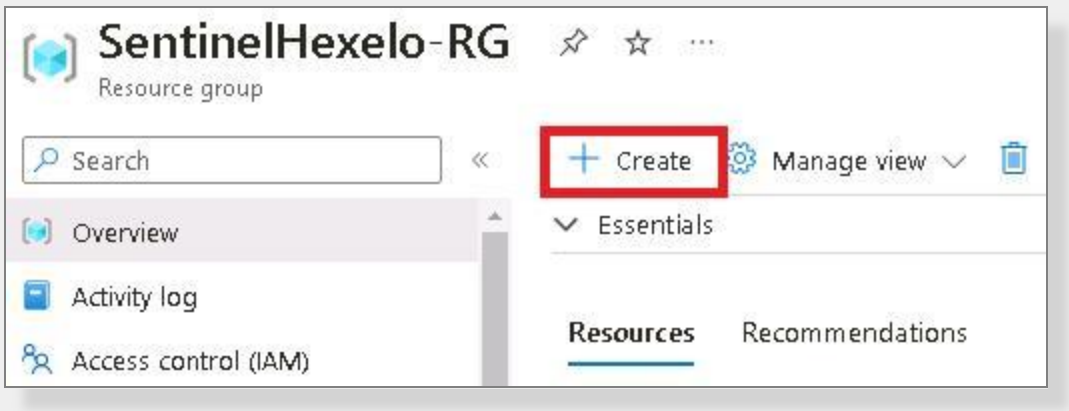
A resource group is a logical container for creating your Azure resources.

It holds all your Azure Resources. A resource group created in a specific region can contain the resources created in other regions.

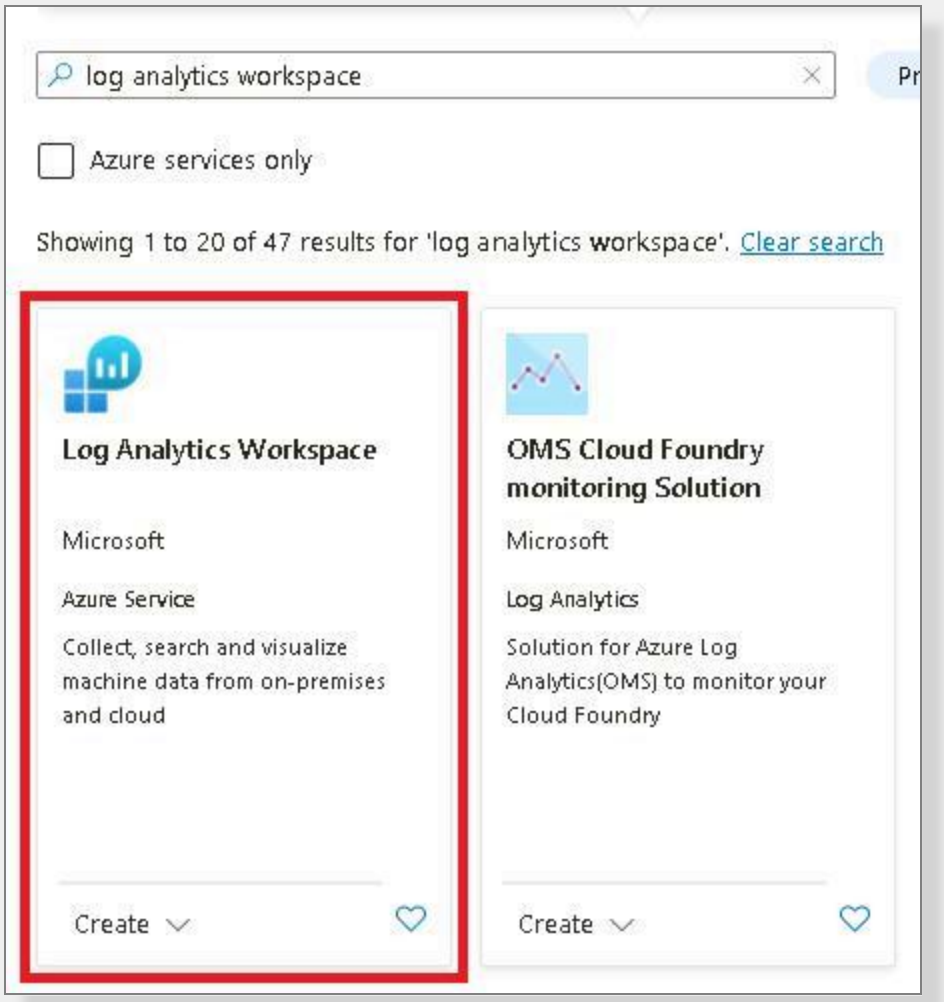
- Create a Log Analytics Workspace named T SentinelHexelo-LAW in the **SentinelHexelo** resource group, by using **US East** as the Region.

Expand this hint for guidance on creating a log analytics workspace.

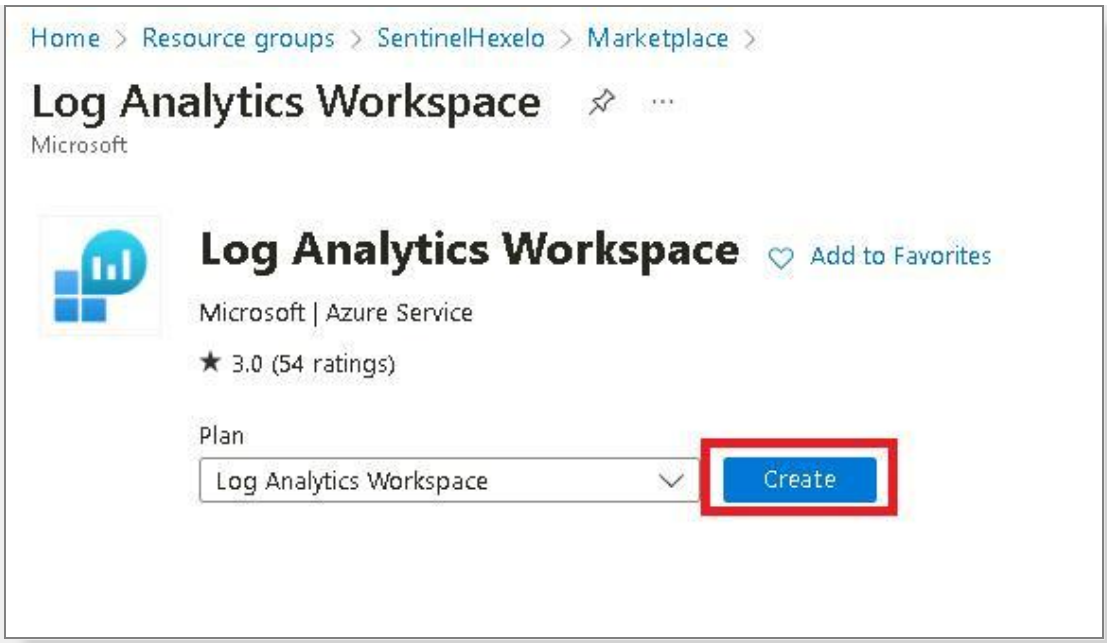
- On the Resource groups page, select **SentinelHexelo-RG**.
- On the SentinelHexelo-RG overview page, select **Create**.



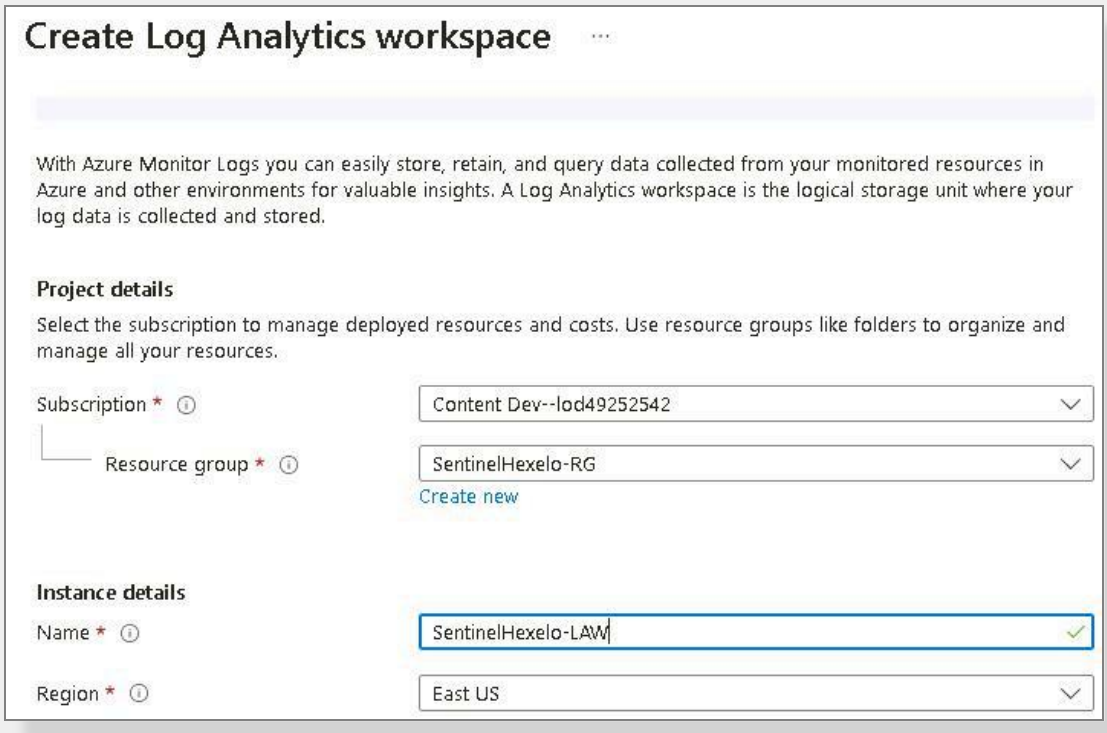
- On the Azure Marketplace page, in Search resources, services, and docs (G+/), search for and select T Log Analytics Workspace.



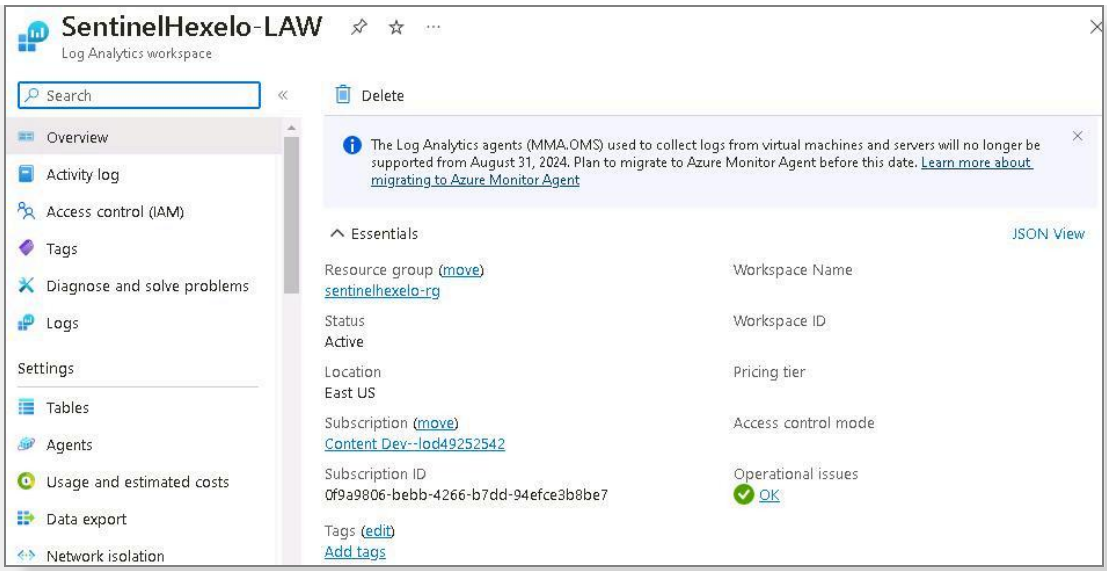
- On the Log Analytics Workspace page, select **Create**.



- On the Create Log Analytics workspace page, on the Basics tab, select your Subscription, and then in Resource group, select **SentinelHexelo-RG**.
- In Instance details, in Name, enter T SentinelHexelo-LAW, and then in Region, select **US East**.



- Select Review + Create, verify that the log analytics workspace has passed validation, and then select **Create**.
- Once deployment is complete, select **Go to resource**.



Want to learn more? Review the documentation on creating a log analytics workspace.

⚠ Deployment may take a few minutes. Select **Refresh** if the new workspace is not listed after a few minutes.

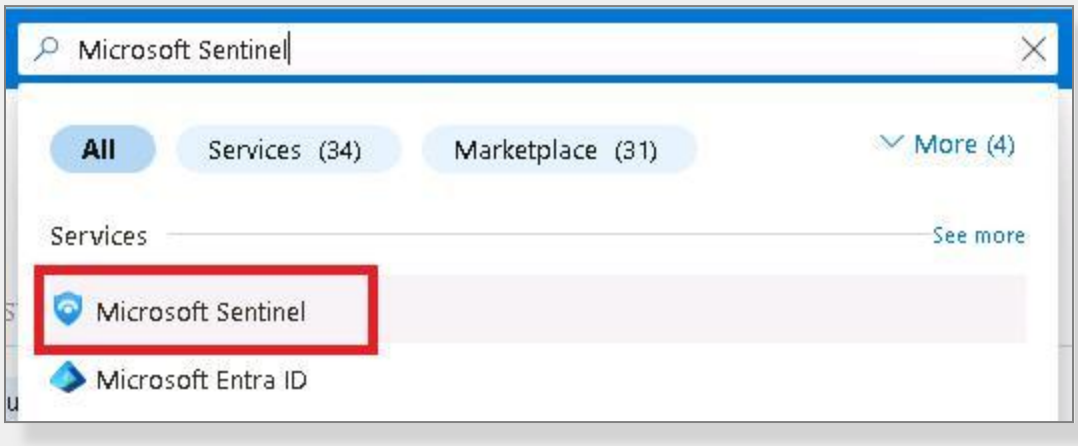
An Azure Log Analytics Workspace is a unique environment for log data from Azure Monitor and other Azure services, such as Microsoft Sentinel and Microsoft Defender for Cloud.

Each workspace has its own data repository and configuration but might combine data from multiple services.

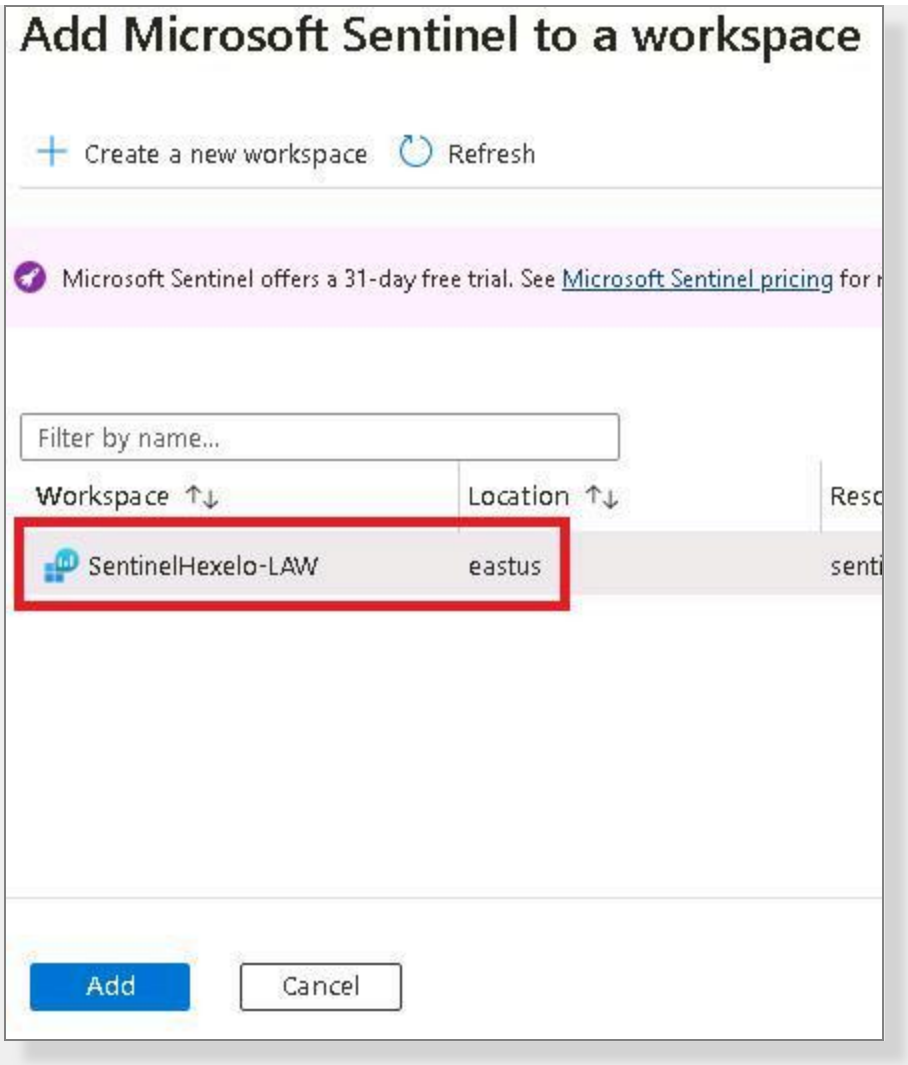
- Add Microsoft Sentinel to the **SentinelHexelo-LAW** workspace.

Expand this hint for guidance on creating a Microsoft Sentinel.

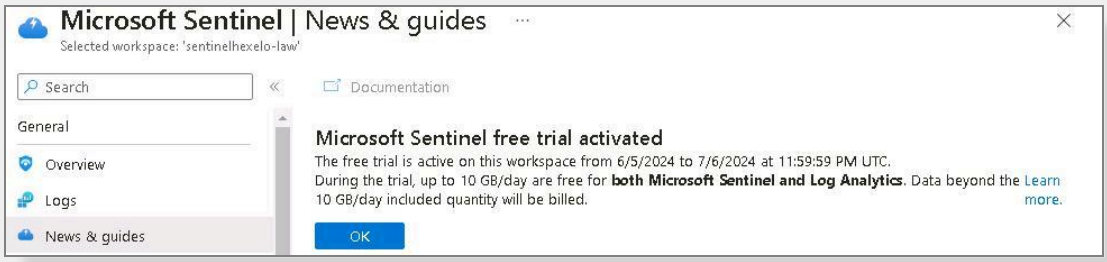
- On the SentinelHexelo-LAW overview page, in Search resources, services, and docs (G+/), search for and select T Microsoft Sentinel.



- On the Microsoft Sentinel home page, select **Create Microsoft Sentinel**.
- On the Add Microsoft Sentinel to a workspace page, in Workspace, select **SentinelHexelo-LAW**, and then select **Add**.



- On the Microsoft Sentinel free trial activated dialog, select **OK**.



Want to learn more? Review the documentation on creating a Microsoft Sentinel instance.

Microsoft Sentinel is a scalable, cloud-native Security Information and Event Management (SIEM) system.

It provides an intelligent and comprehensive solution for SIEM and Security Orchestration, Automation, and Response (SOAR).

Check your work

Verify

Create and connect a new virtual machine

Hints Enabled

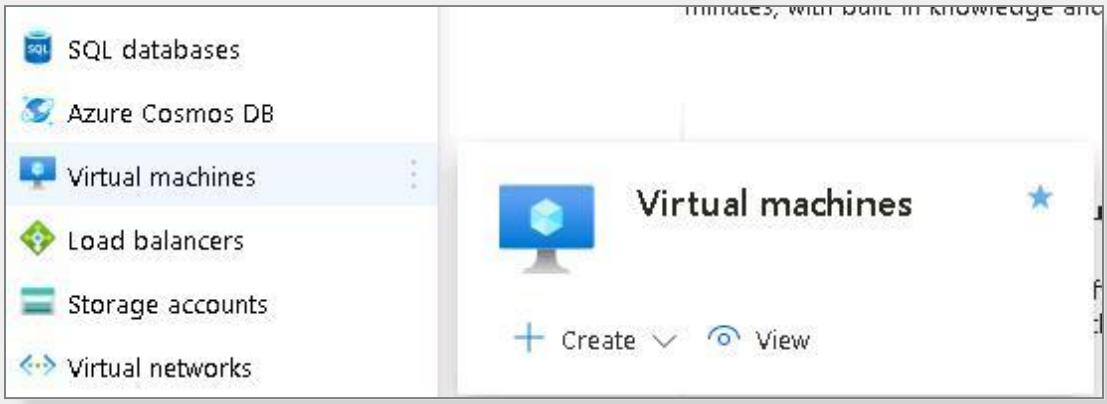
No Yes

- Create a virtual machine by using the following table:

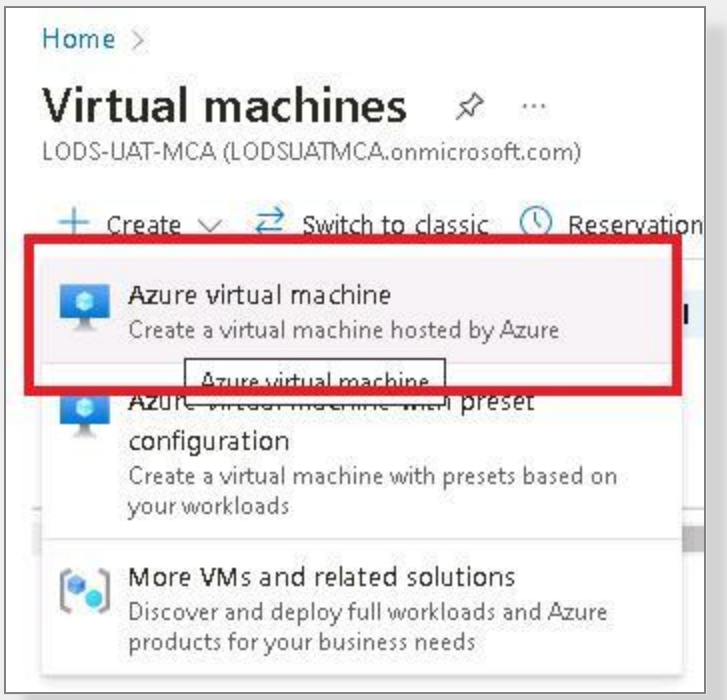
Setting	Value
Resource group	**SentinelHexelo-RG**
Virtual machine name	T SentinelHexelo-VM
Region	**East US**
Availability options	**No infrastructure redundancy required**
Security type	**Standard**
Image	**Windows 11 Pro, version 22H2 - x64 Gen2**
Size	T Standard_E2s_v3, 16 GiB memory
Username	T SentinelHexeloAdmin
Password/Confirm password	T SentinelPassw0rd!
Licensing	**Enabled**
NIC network security group	**Advanced**

Expand this hint for guidance on creating a virtual machine.

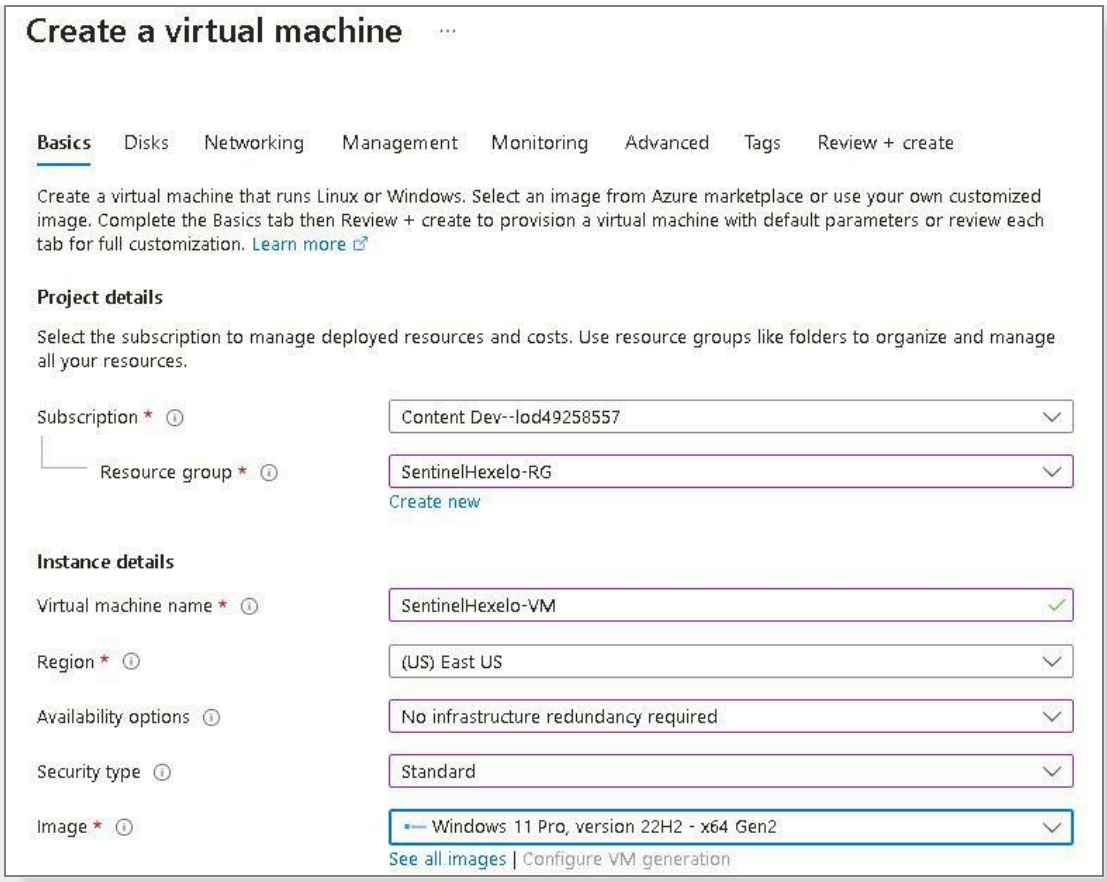
- On the Microsoft Sentinel | News & guides page, select the hamburger menu in the upper left, and then select **Virtual machines**.



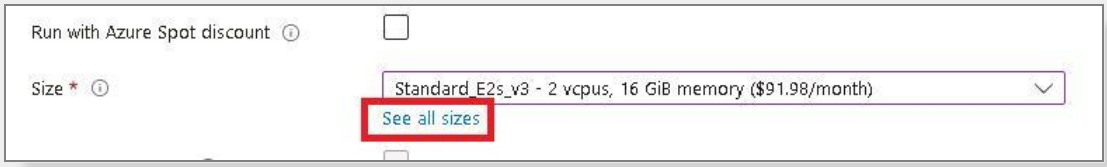
- On the Virtual machines home page, select Create, and then select **Azure virtual machine**.



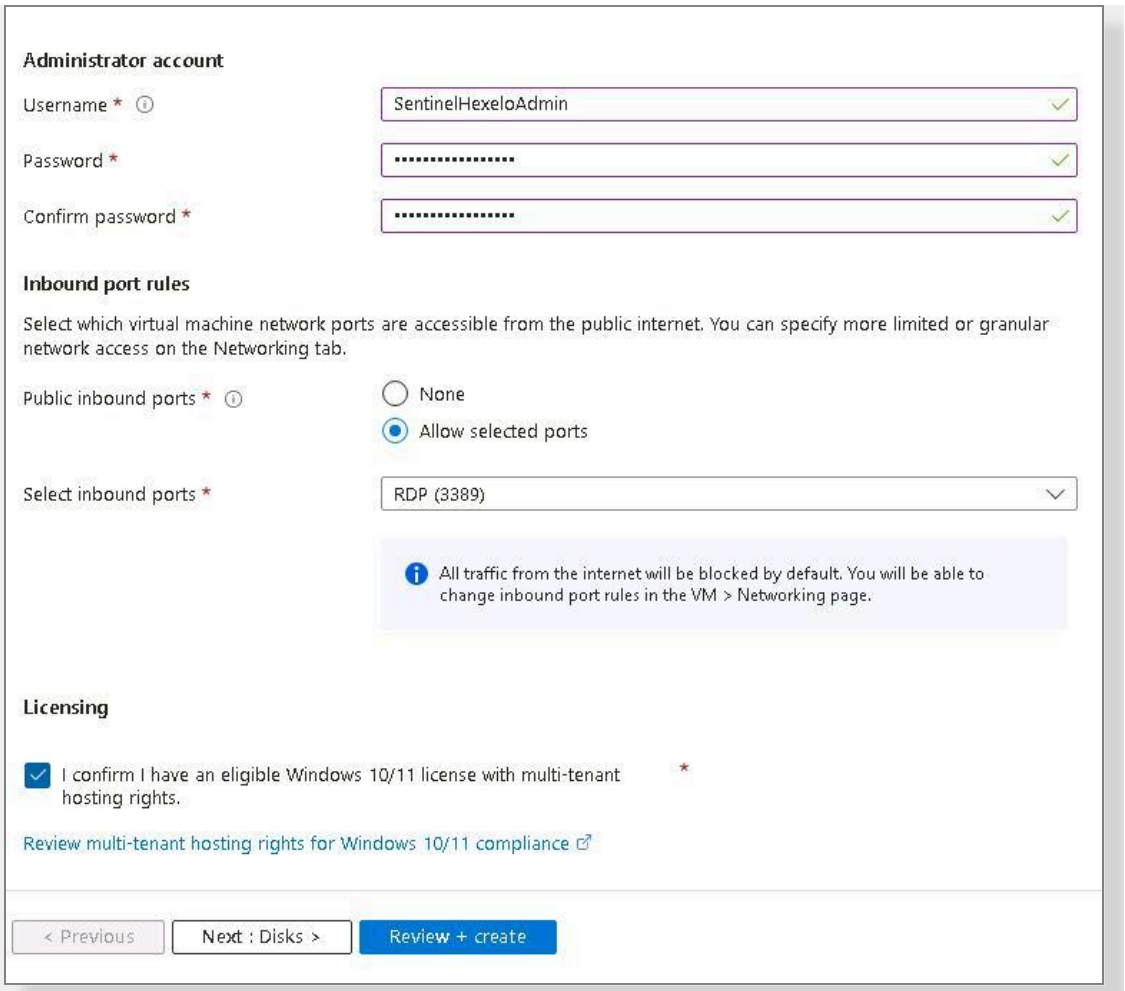
- On the Create a virtual machine page, on the Basics tab, select your subscription, and then in Resource group, select **SentinelHexelo-RG**.
- In Virtual machine name, enter T SentinelHexelo-VM, and then in Region, select **East US**.
- In Availability options, select **No infrastructure redundancy required**.
- In Security type, select **Standard**.
- In Image, select **Windows 11 Pro, version 22H2 - x64 Gen2**.



- In Size, select **See all sizes**, and then search for and select T Standard_D2s_v3 - 2 vcpus, 8 GiB memory.



- In Username, enter T SentinelHexeloAdmin, and then in Password and Confirm password, enter T SentinelPassw0rd!.
- In Licensing, enable the *I confirm I have an eligible Windows 10/11 license with multi-tenant hosting rights* checkbox, and then select **Next:Disks>**.



- On the Disks tab, review the default settings, and then select **Next: Networking>**.

Want to learn more? Review the documentation on creating a virtual machine.

Azure Virtual Machines (VMs) are powerful and flexible cloud computing resources offered by Microsoft Azure.

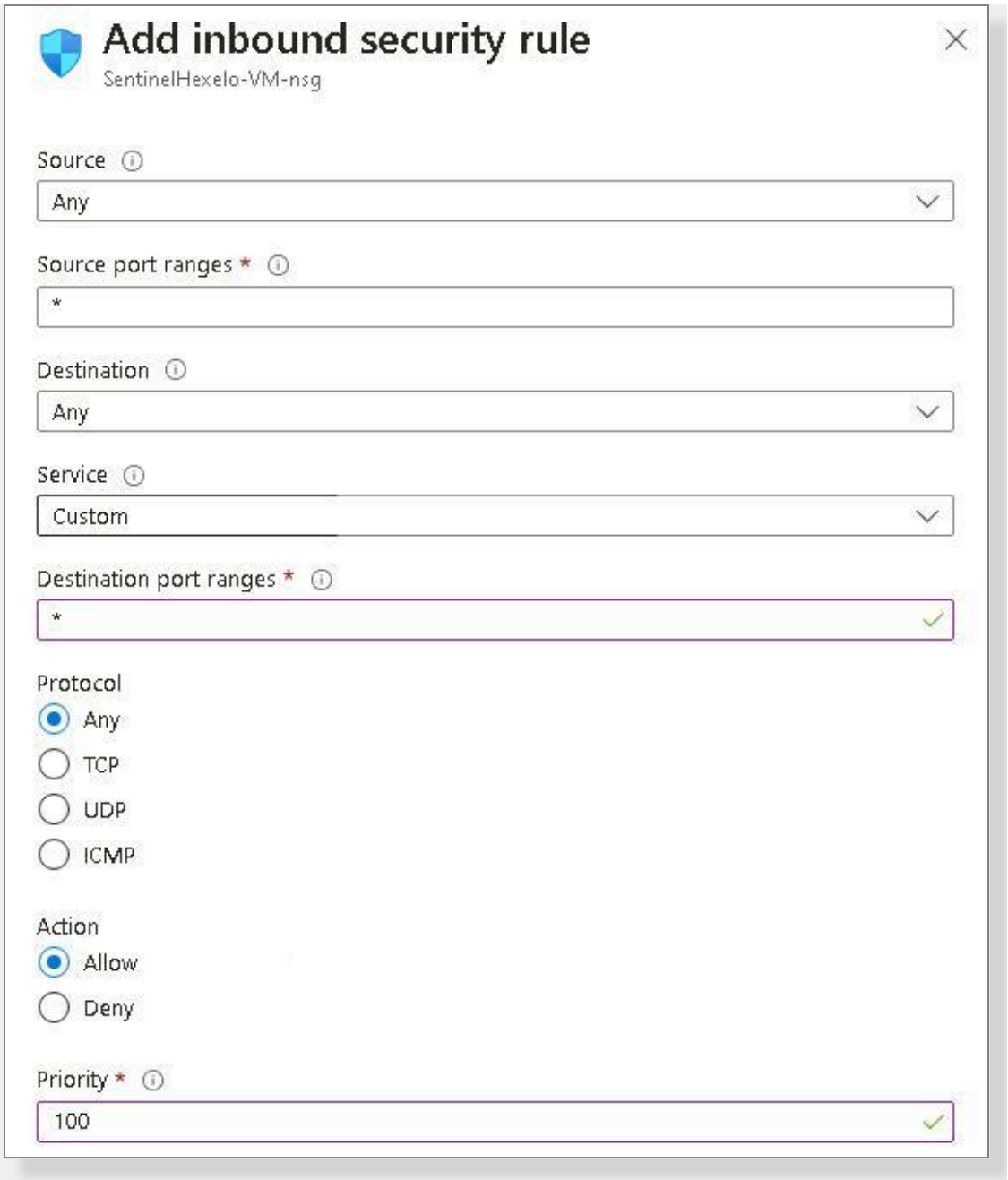
They allow users to create and manage virtual machines in the Azure cloud, providing scalability, reliability, and security without the burden of managing physical infrastructure. Whether for development and testing, running applications in the cloud, or extending your datacenter, Azure VMs offer flexibility and efficiency for various workloads.>

- Create a Network security group named T SentinelHack-DANGER, by using an Inbound rule with a Priority of T 100, and the following port ranges: T *

Expand this hint for guidance on creating an inbound rule.

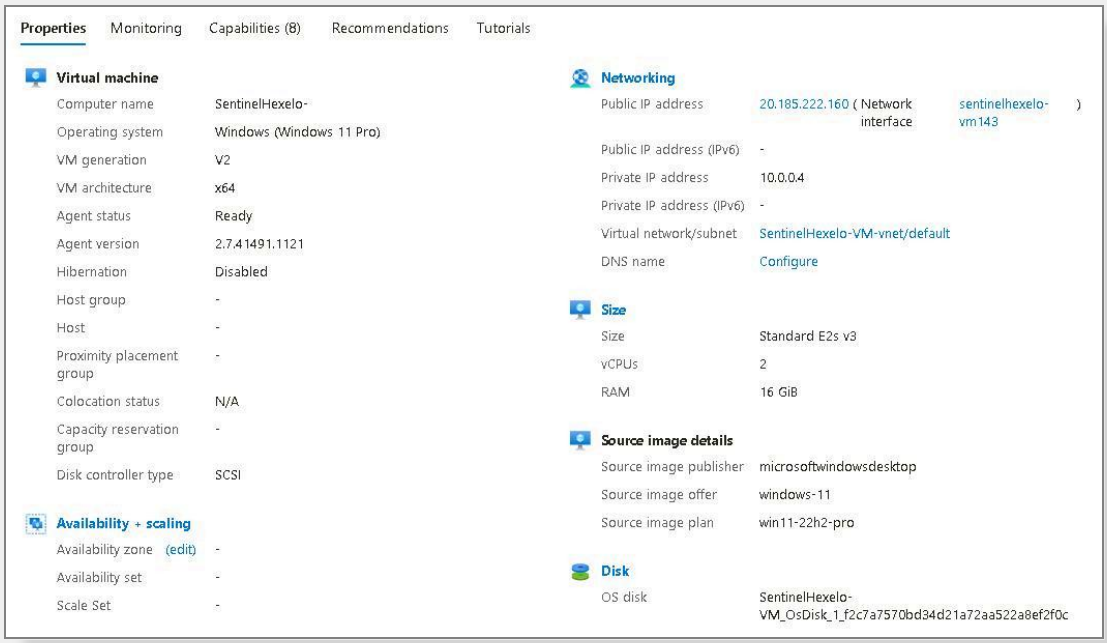
- On the Networking tab, in Network interface, in NIC network security group, select **Advanced**.
- In Configure network security group, select **Create new**.

- On the Create network security group page, in Inbound rules, select the Recycle icon to delete the current Inbound rule.
- In Inbound rules, select **Add an inbound rule**, and then on the Add inbound security rule blade, in Destination port ranges, enter T *.
- In Priority, enter T 100.



- In Name, enter T SentinelHack-DANGER, and then select **Add**.

- On the Create network security group, select **OK**, select **Review + create**, and then select **Create**.



Want to learn more? Review the documentation on creating an inbound rule.

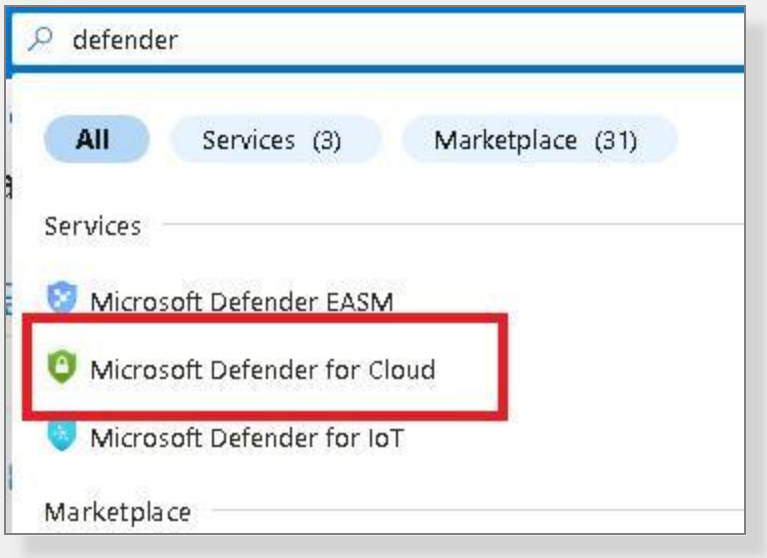
Microsoft Sentinel inbound rules, also known as analytics rules, are designed to help security teams discover threats and anomalous behaviors across their digital environment.

These rules search for specific events or sets of events, alerting the team when certain event thresholds or conditions are met. They generate incidents for the Security Operations Center (SOC) to triage and investigate, and respond to threats with automated tracking and remediation processes. Users can create custom analytics rules from scratch or customize templates provided in the Content hub to fit their specific scenarios. This ensures full security coverage for the environment.

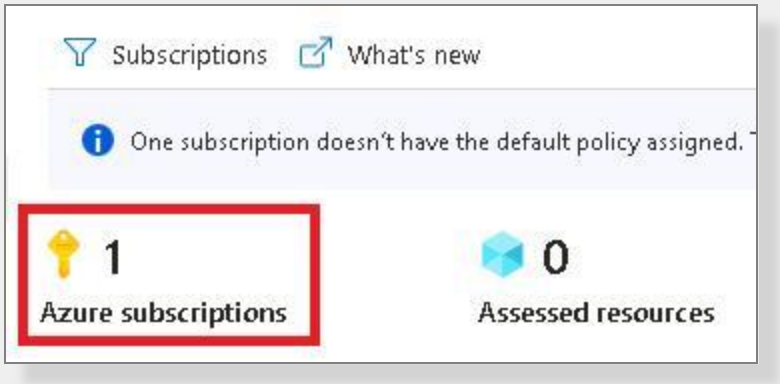
- By using the SentinelHexelo-LAW workspace, enable the Servers Microsoft Defender plan, turn on Servers, and then set Data collection to collect all events.

Expand this hint for guidance on enabling Microsoft Defender.

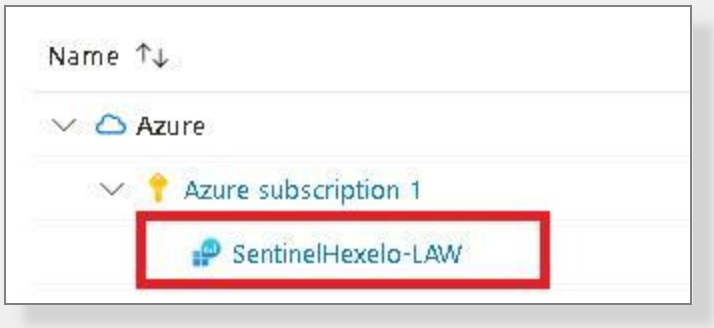
- In Search resources, services, and docs (G+/), search for and select T Microsoft Defender for Cloud.



- On the Microsoft Defender for Cloud | Overview page, select **Azure subscriptions**.

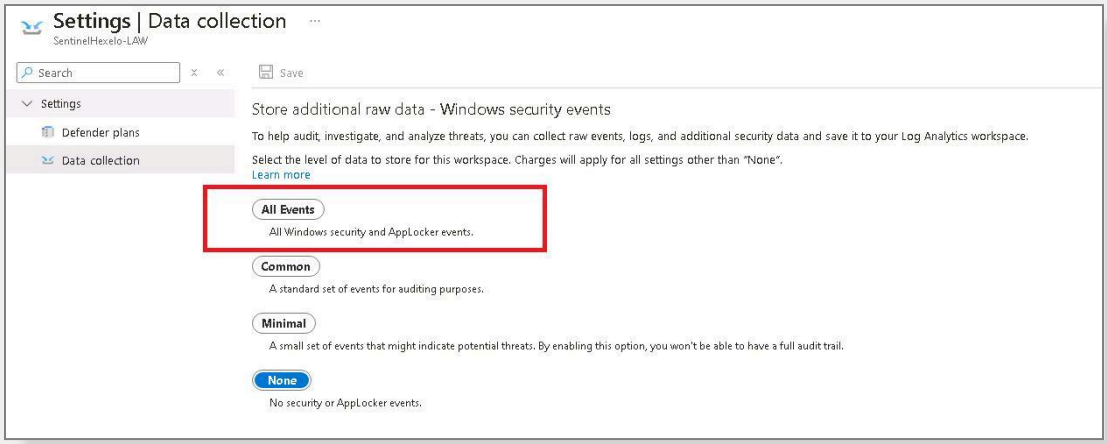


- On the Environment settings page, expand the subscription, and then select the **SentinelHexelo-LAW** workspace.



- On the SentinelHexelo-LAW Settings | Defender plans page, in Select Defender plan, set the **Servers** plan to **On**, and then select **Save**..

- In Settings, select **Data collection**, select **All Events**, and then select Save.



Want to learn more? Review the documentation on enabling Microsoft Defender.

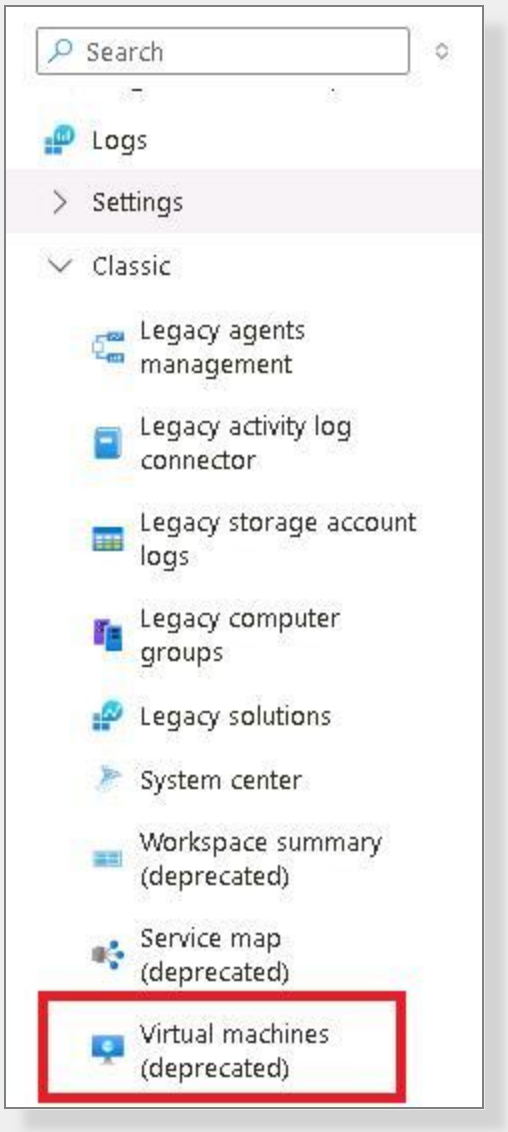
Microsoft Defender for Cloud is a cloud-native application protection platform (CNAPP) that provides robust security measures to protect cloud-based applications from various cyber threats and vulnerabilities.

It combines the capabilities of a development security operations (DevSecOps) solution, a cloud security posture management (CSPM) solution, and a cloud workload protection platform (CWPP). This platform helps incorporate good security practices early during the software development process, allowing you to protect your code management environments and your code pipelines. It also provides insights into your development environment security posture from a single location.

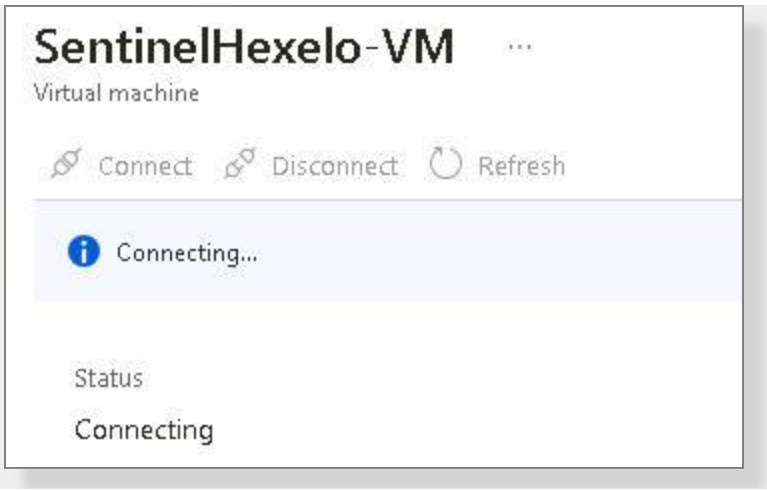
- Connect the **SentinelHexelo-LAW** workspace to the **SentinelHexelo-VM** virtual machine.

Expand this hint for guidance on connecting a log analytics workspace to a virtual machine.

- On the Azure Marketplace page, in Search resources, services, and docs (G+/), search for and select T Log Analytics Workspace.
- Select the SentinelHexelo-LAW, expand Classic, and then select **Virtual machines**.



- On the SentinelHexelo-LAW | Virtual machines page, select SentinelHexelo-VM, and then on the SentinelHexelo-VM page, select **Connect**.



Want to learn more? Review the documentation on connecting a log analytics workspace to a virtual machine.

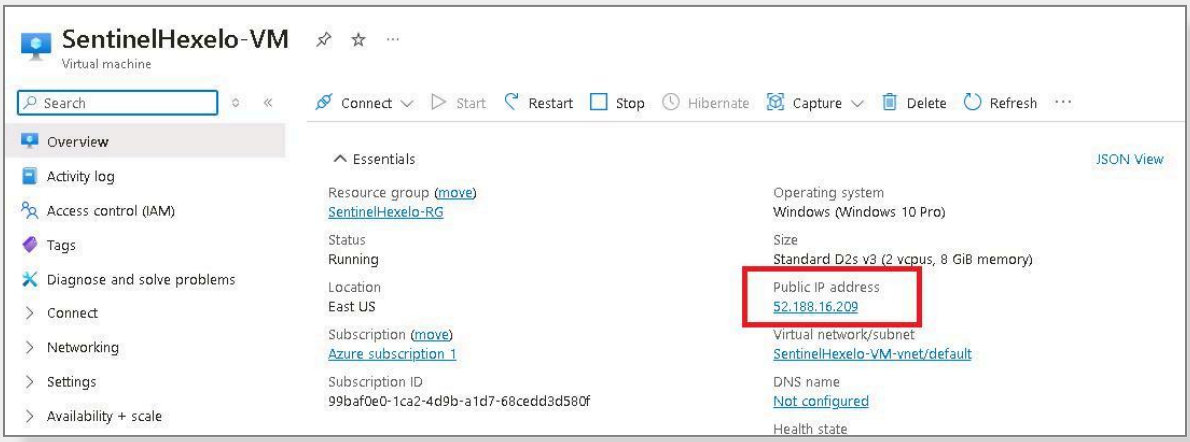
Connecting a Log Analytics workspace to a virtual machine in Microsoft Sentinel involves installing the Log Analytics agent on the machine that will be generating the logs.

From the Log Analytics workspace navigation menu, you select Virtual machines. In the Virtual machines blade, you select a virtual machine to install the agent on, and then select Connect. You repeat this step for each VM you wish to connect. This process allows the Log Analytics agent to collect data in text files of nonstandard formats from both Windows and Linux computers, and these logs can then be analyzed and monitored in Microsoft Sentinel.

- Locate the SentinelHexelo-VM Public IP address, and then enter it in the following textbox:

SentinelHexelo-VM Public IP address

The following image shows the VM Overview page with the Public IP address selected.



Verify

Connect to the Remote Desktop

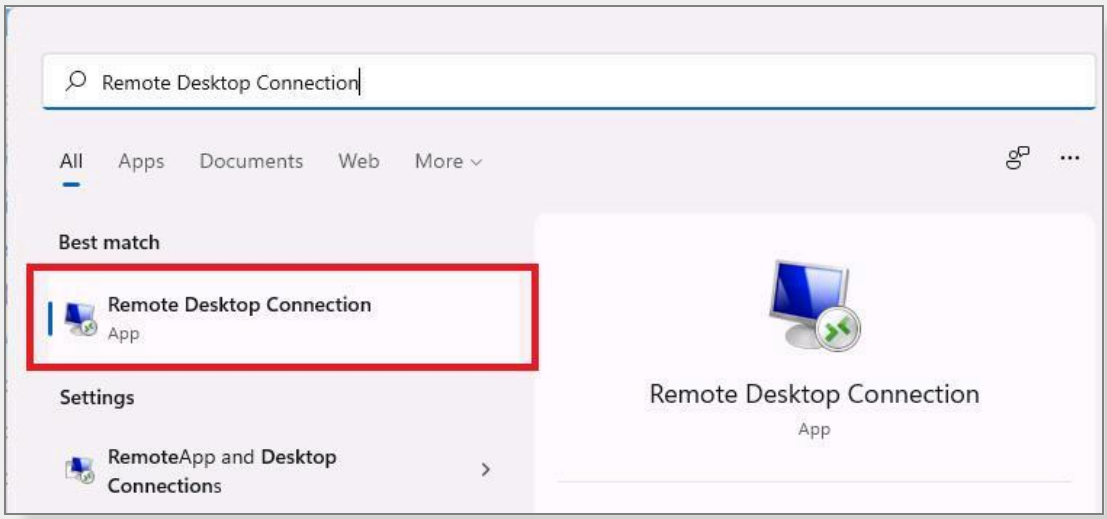
Hints Enabled

No  Yes

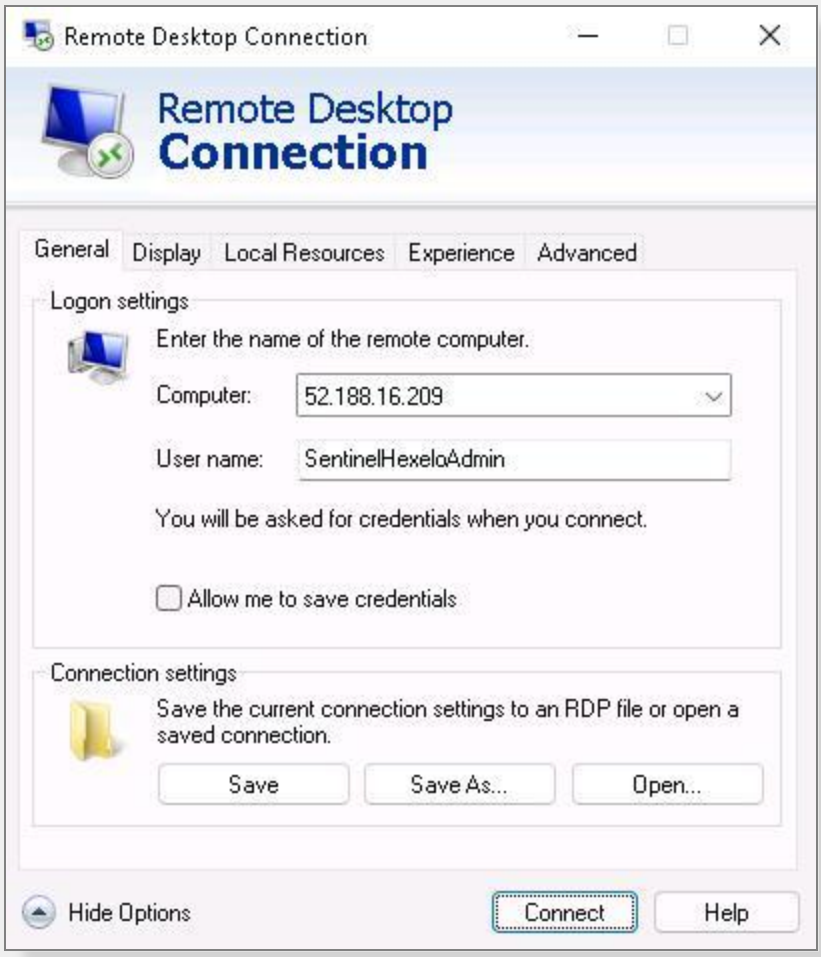
- Open the SentinelHexelo-VM by using **Remote Desktop Connection**.

Expand this hint for guidance on connecting to a virtual machine by using Remote Desktop Connection.

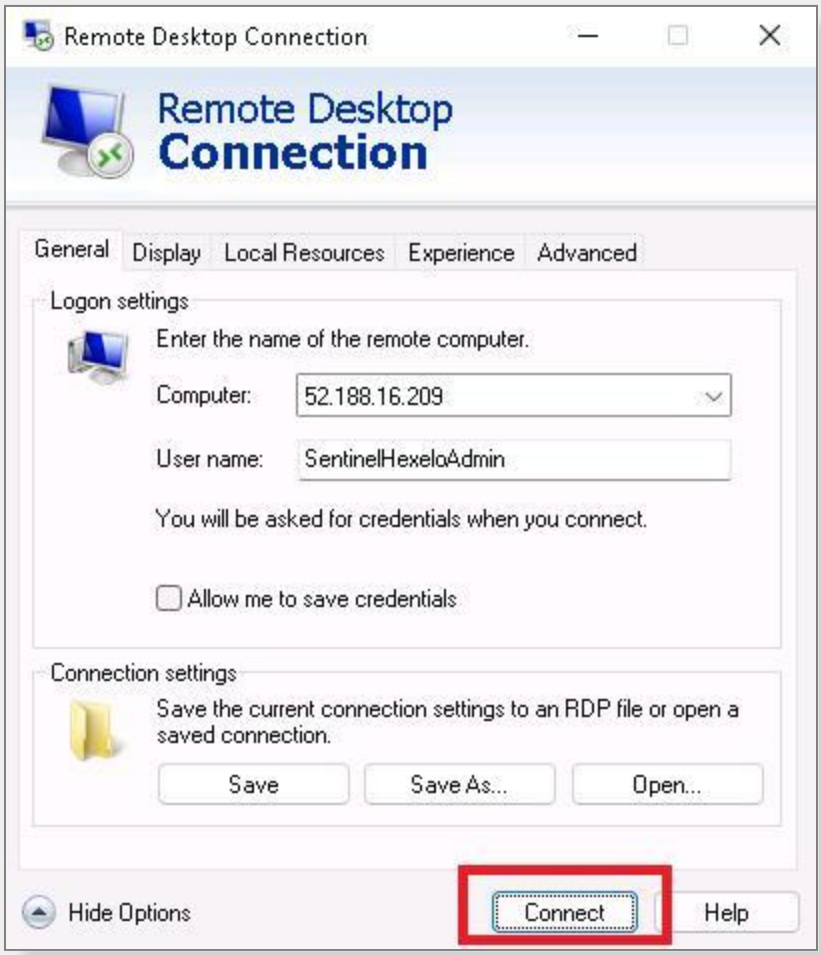
- On the **Windows 11** desktop, select the Search icon, and then enter T Remote Desktop Connection.



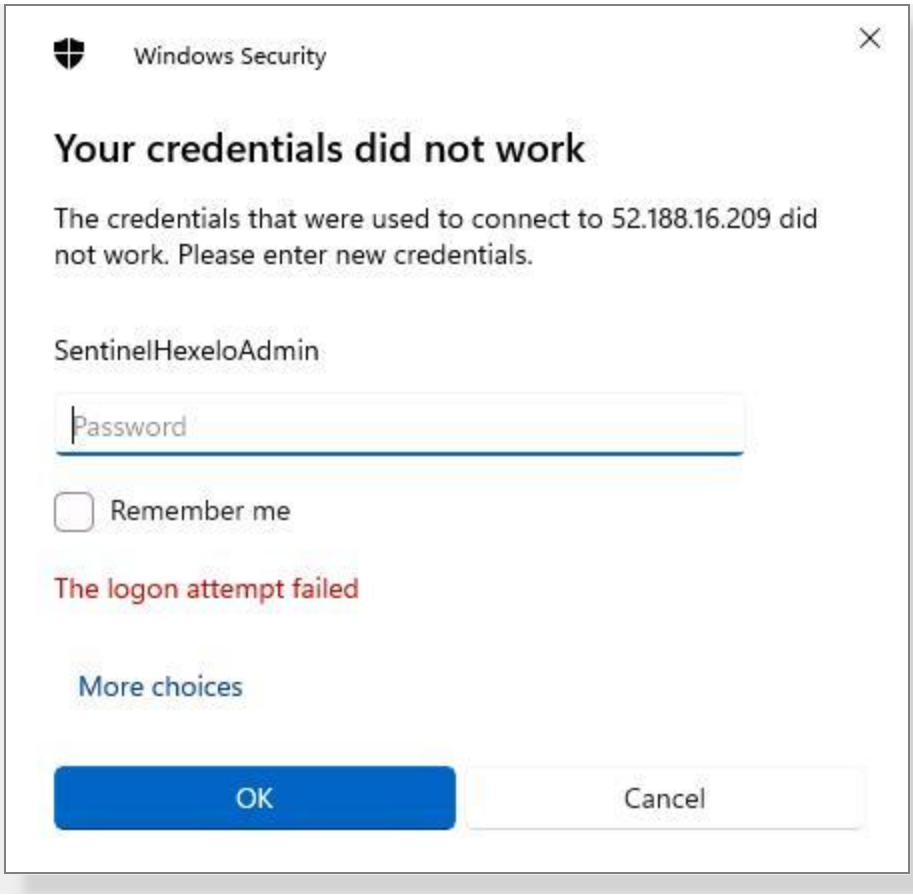
- On the Remote Desktop Connection dialog, in Computer, enter SentinelHexelo-VM IP address, in Username, enter T SentinelHexeloAdmin, and then select **Connect**.



- On the Enter your credentials dialog, select **More choices**, and then select **Use a different account**.
- In Username, enter T WrongUser, in Password, enter T Wrongpassword, and then select **OK**.



- On the Enter your credentials dialog, enter T Password, and then select **OK**.



Want to learn more? Review the documentation on using Remote Desktop Connection

⚠ The logon attempt should fail.

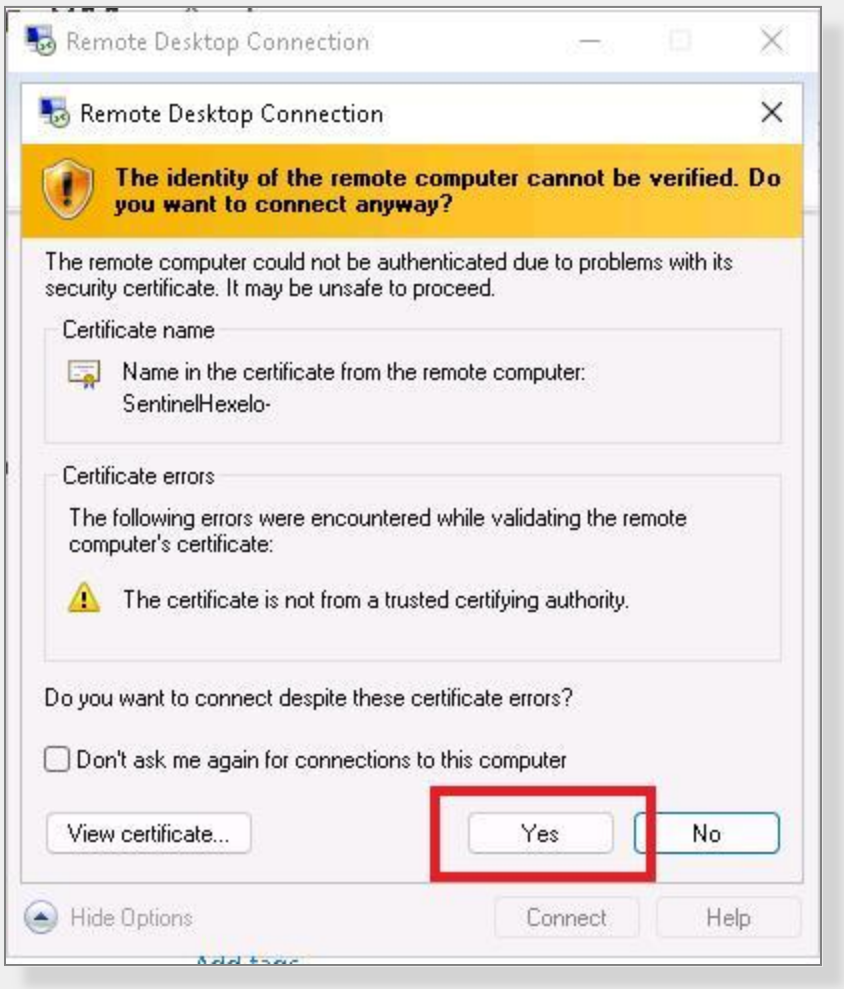
Remote Desktop Connection is a feature on Windows devices that allows a user to remotely control another computer.

It works by transmitting the screen, mouse, and keyboard inputs from one device to another, enabling users to access their desktop, open and edit files, and use applications as if they were physically at the remote computer. During a remote session, the remote computer gets logged out, and all control is given to the client device. This is particularly useful for tech support specialists who frequently employ remote desktop connectivity to troubleshoot live fixes on a client's machine.

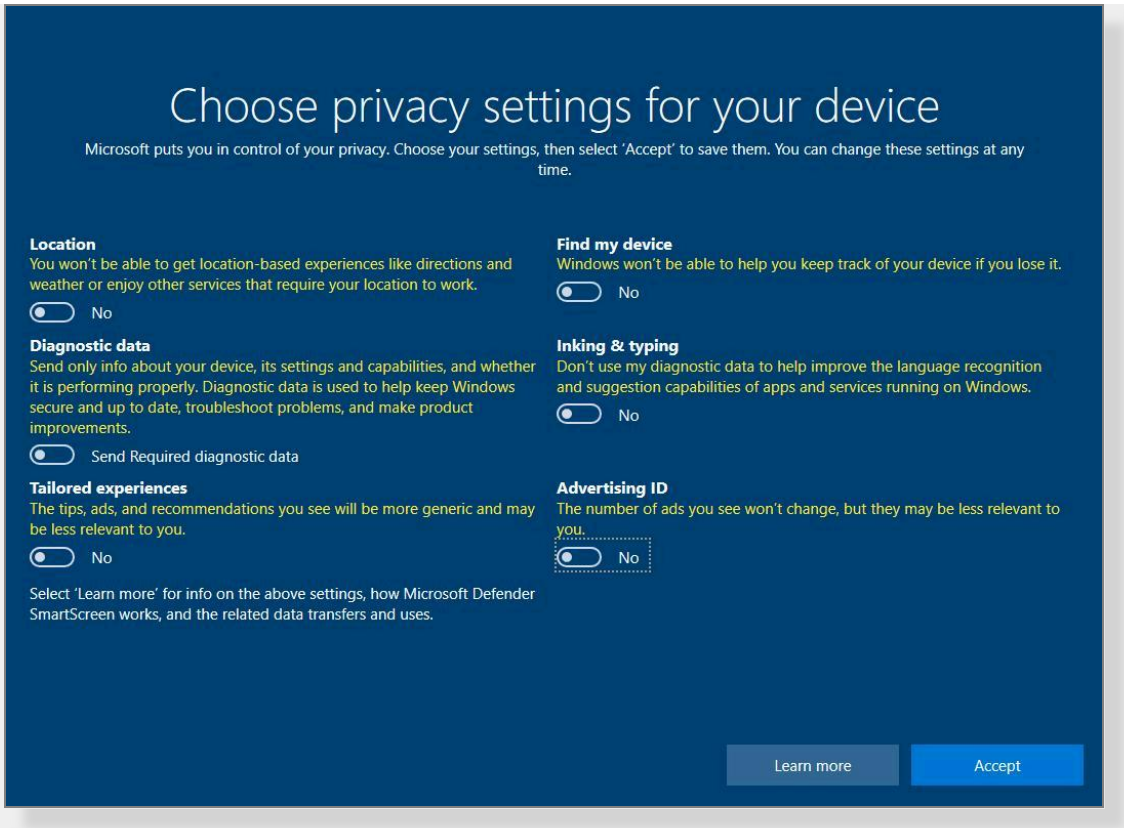
- Login to **SentinelHexelo-VM** by using T Intruder as the username and T X1X2X3X4, as the password.
- Login to **SentinelHexelo-VM** by using T Attacker as the username and T ABCD1234, as the password.
- Login to **SentinelHexelo-VM** by using T SentinelHexeloAdmin as the username and T SentinelPassw0rd!, as the password.

Expand this hint for guidance on logging in to a virtual machine.

- In Username, enter T SentinelHexeloAdmin, in Password, enter T SentinelPassw0rd!, and then select **OK**.
- On the *The identity of the remote computer cannot be verified. Do you want to connect anyway?* dialog, select **Yes**.



- Dismiss any popup screens, and then minimize the **SentinelHexelo-VM** Remote Desktop window.



Want to learn more? Review the documentation on logging in to a virtual machine by using Remote Desktop Connection.

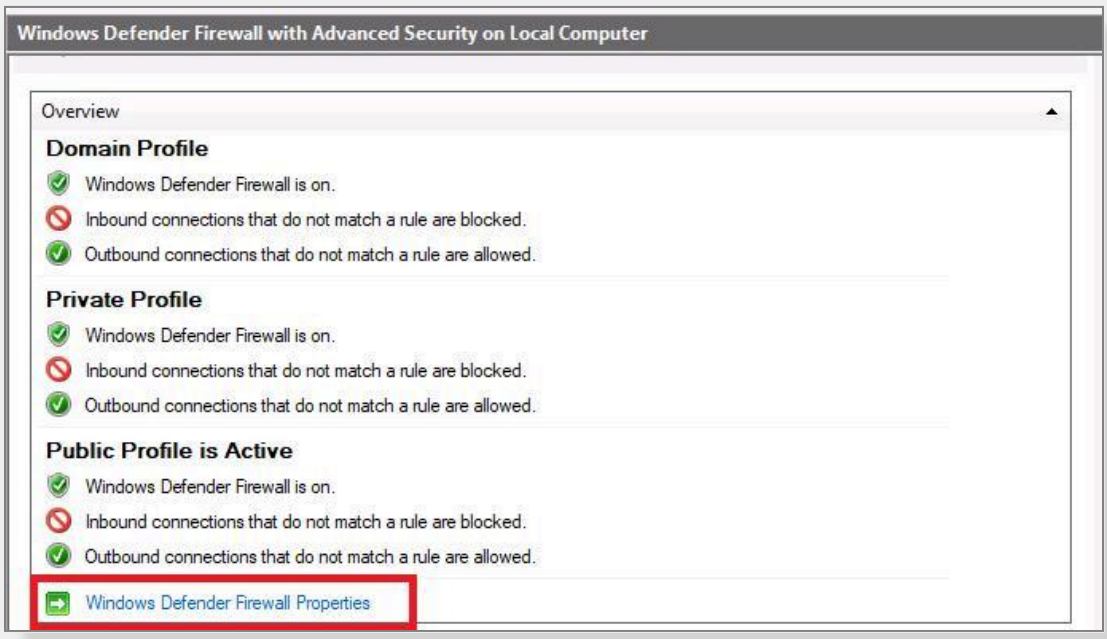
Capturing login values in an event log involves tracking specific events related to user logins.

These events are logged with different logon types, such as interactive (type 2), network (type 3), batch (type 4), and service (type 5). Each logon type represents a different method of user authentication. For instance, an event with logon type 2 occurs when a user logs on to a computer locally, while logon type 3 is used when a user or computer logs on to a computer from the network.

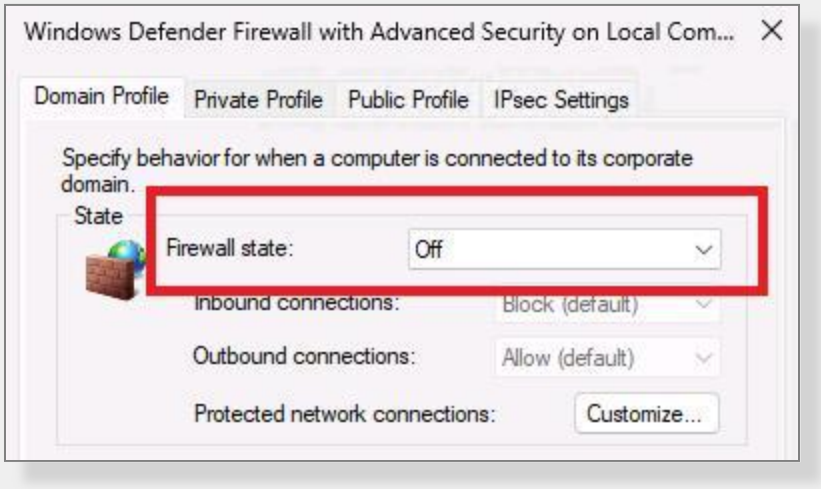
- Disable Windows Defender Firewall for the **Domain Profile**, **Private Profile**, and the **Public Profile** on the SentinelHexelo-VM virtual machine

Expand this hint for guidance on disabling Windows Defender firewall.

- On the **SentinelHexelo-VM** desktop, select the Search icon, and then enter T wf.msc.
- On the Windows Defender Firewall with Advanced Security page, in Overview, select **Windows Defender Firewall Properties**.



- On the Windows Defender Firewall dialog, on the Domain Profile tab, in Firewall state, select **Off**.



- On the Private Profile tab, in Firewall state, select **Off**.
- On the Public Profile tab, in Firewall state, select **Off**, select **Apply**, and then select **OK**.

Want to learn more? Review the documentation on disabling Windows Defender firewall.

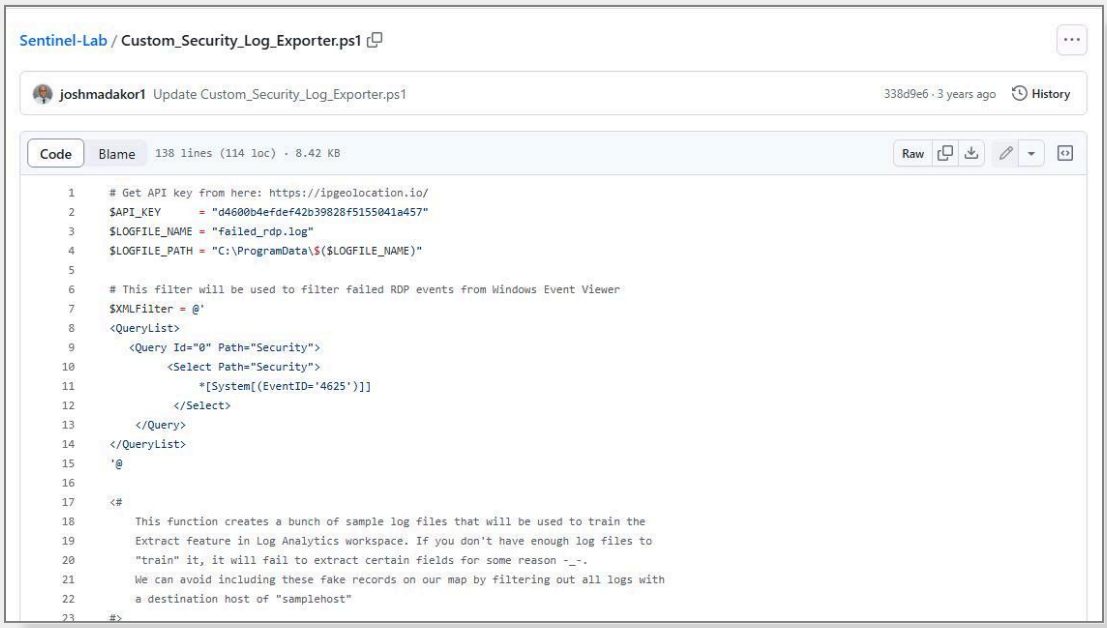
Windows Defender Firewall is a built-in security feature in all Windows computers that helps protect your device by filtering network traffic.

It permits or denies programs on a computer from accessing network or Internet resources, and allows or blocks connections to and from other computers on a network. The firewall can be configured based on several criteria, including source and destination IP address, IP protocol, or source and destination port number. It also works with Network Location Awareness to apply security settings appropriate to the types of networks to which the device is connected. Thus, Windows Defender Firewall provides an additional layer of defense to the defense-in-depth model, increasing manageability and decreasing the likelihood of a successful attack.

- Copy the GitHub **Custom_Security_Log_Exporter**.

Expand this hint for guidance on using the Custom_Security_Log_Exporter.

- In Edge, open a new tab, and then enter T https://github.com/joshmadakor1/Sentinel-Lab/blob/main/Custom_Security_Log_Exporter.ps1.



- In the Github Code Window, select the **Copy Raw file** icon.

Want to learn more? Review the documentation on using the Custom_Security_Log_Exporter.

The *Custom_Security_Log_Exporter* is a PowerShell script used in Microsoft Sentinel for parsing out Windows Event Log information related to failed Remote Desktop Protocol (RDP) attacks.

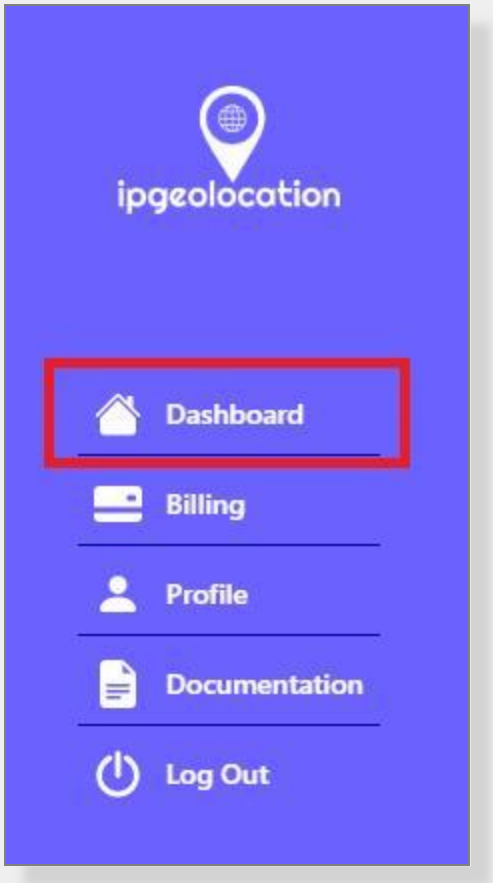
It uses a third-party API to collect geographic information about the attacker's location. The script filters failed RDP events from the Windows Event Viewer and writes them to a log file. It also creates sample log files to train the Extract feature in the Log Analytics workspace. This allows for the visualization of live attacks from around the world, including the geolocation information of the attackers.

- Sign up for a free ipgeolocation account, and then copy the **ipgeolocation API**.

Expand this hint for guidance on using ipgeolocation.

- In Edge, open a new tab, and then enter T https://ipgeolocation.io.

- Select **Sign up**, enter the User name, Email, and Password of your choosing, verify the reCAPTCHA, and then select **Sign Up**.
- Once you are logged in, select **Dashboard**.



- On the Developer|API Subscription page, locate the API Keys.

Want to learn more? Review the documentation on using ipgeolocation.

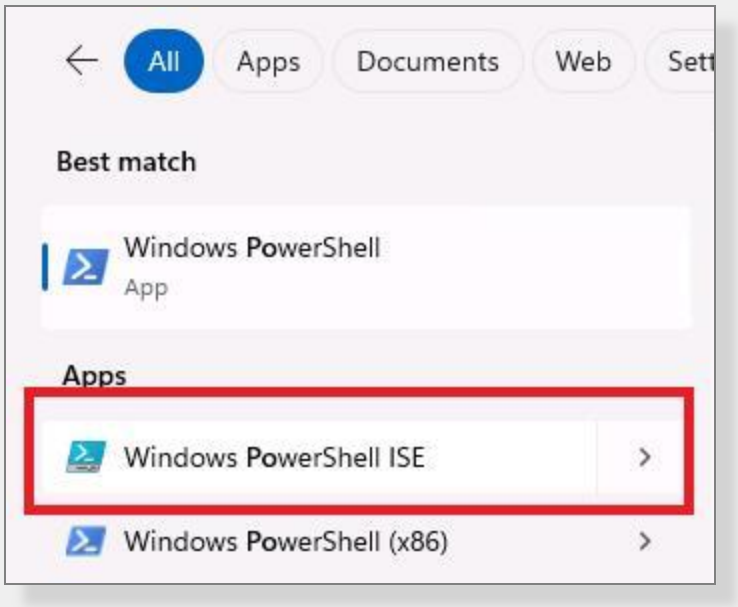
IP Geolocation is a technique used to estimate the geographic location of an internet-connected device using its IP address.

This method doesn't provide exact location details, but it can give a general idea of the city, state, or country where the device is located. The process involves databases that map IP addresses to geographical locations, which are maintained by various organizations. These databases are updated regularly to accommodate changes in IP allocations. It's important to note that due to factors like VPN usage and mobile connections, IP geolocation may not always be accurate.

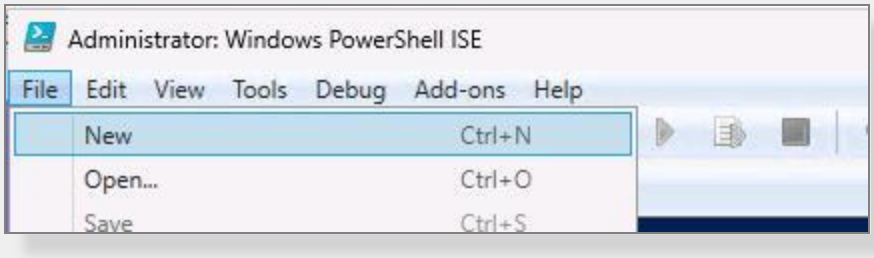
- Replace the Custom_Security_Log_Exporter.ps1 API key with the ipgeolocation API key by using Windows Powershell ISE, and then save the PowerShell script as T Failed RDP.

Expand this hint for guidance on editing Powershell scripts.

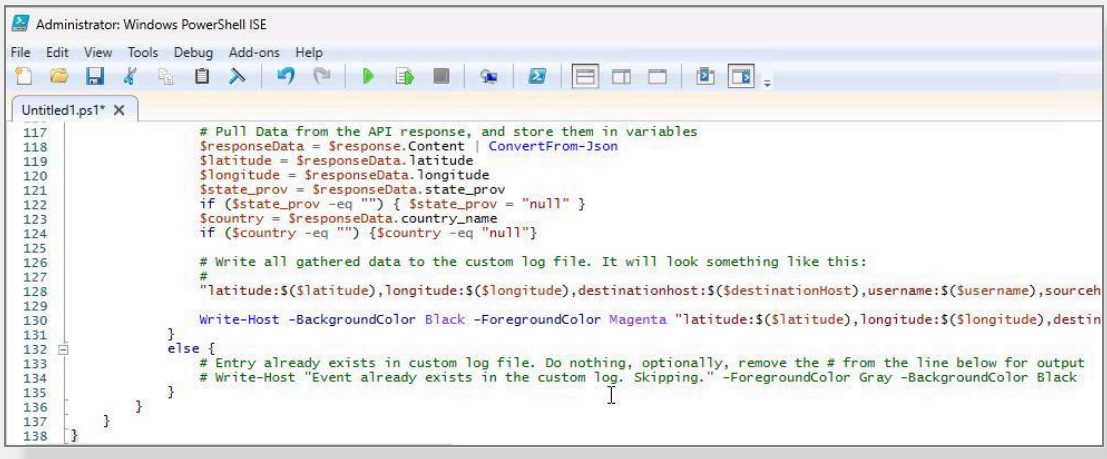
- On the **SentinelHexelo-VM** desktop, select the Search icon, and then enter T Powershell ISE.



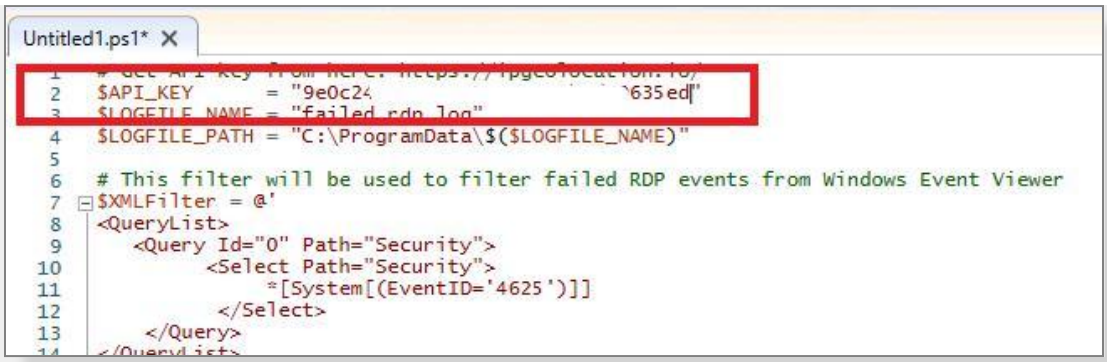
- In the Powershell console, select **File|New**.



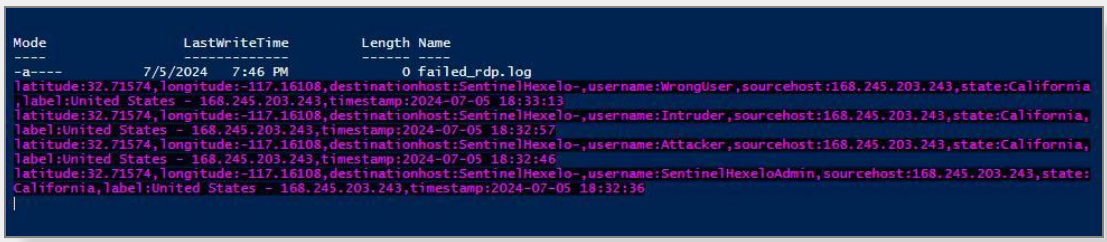
- Select the Sentinel-Lab/Custom_Security_Log_Exporter.ps1 tab, copy the script to the clipboard, and then return to the Powershell console and select **Paste**.



- Select the ipgeolocation tab, copy the Api Keys, and then in the Powershell console, locate the $API_KEY on line 2, and overwrite it with the copied ipgeolocation API key.



- Select the **Run** icon, and then save the Powershell script to your Desktop as T Failed RDP.



-

Want to learn more? Review the documentation on editing Powershell scripts.

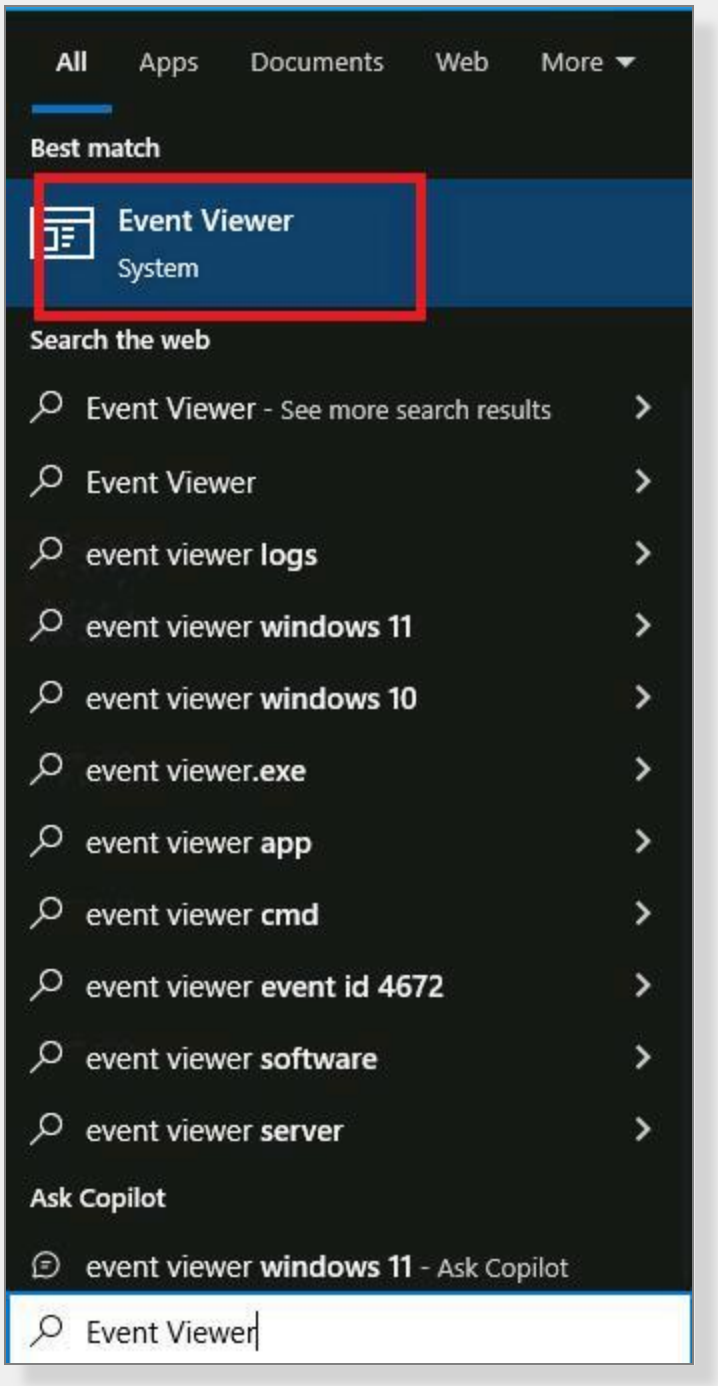
Editing PowerShell scripts involves modifying the text files that contain PowerShell commands and logic.

These scripts, typically with a `.ps1` extension, can be opened and edited in any text editor, but specialized editors like Visual Studio Code or PowerShell ISE provide syntax highlighting and other features that make the process easier. Changes to the script are saved in the file, and the updated script can be run in the PowerShell command line interface to execute the modified commands. It's important to test your scripts after editing to ensure they still function as expected. Always remember to follow best practices for scripting to maintain readability and functionality.

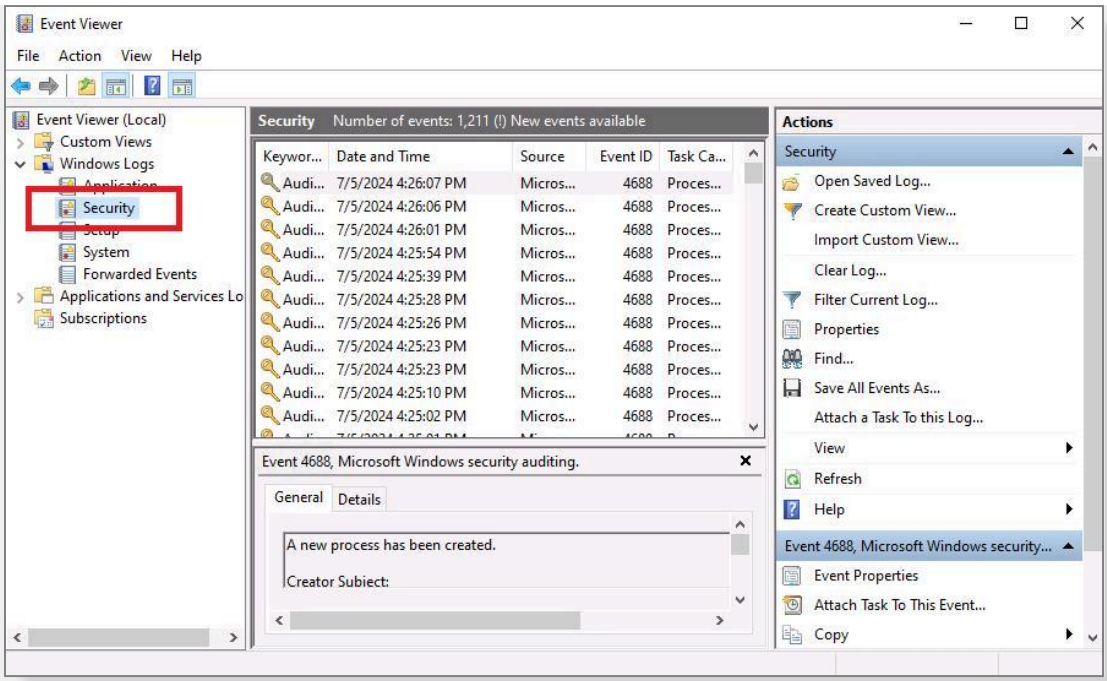
- By using the Event Viewer, search for Audit failures with an Event ID of T 4625.

Expand this hint for guidance on using the Event viewer.

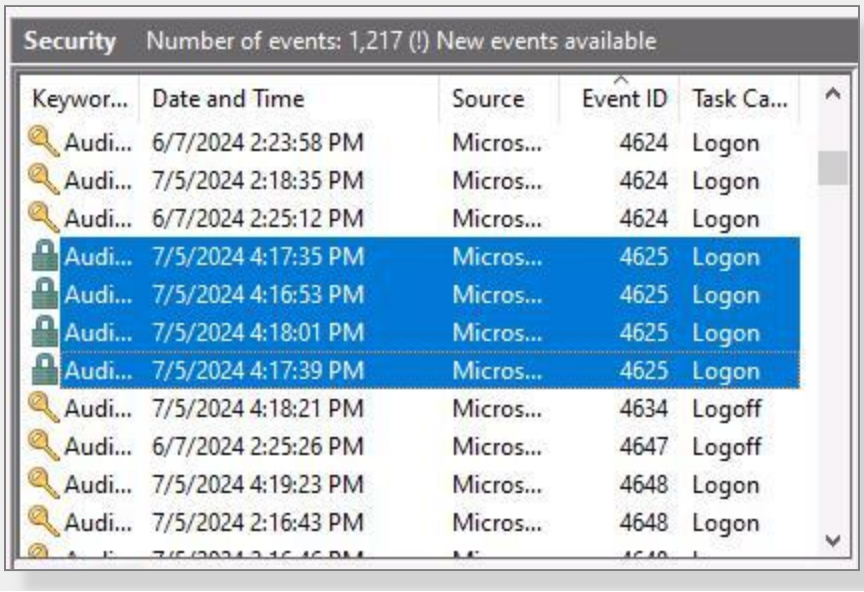
- On the **SentinelHexelo-VM** desktop, select the Search icon, and then enter T Event Viewer.



- On the Event Viewer page, in Event Viewer, in Windows logs, select **Security**.



- In the Security pane, search for Audit failures with an Event ID of T 4625.



Want to learn more? Review the documentation on using the Event viewer.

The Event Viewer is a Microsoft Windows tool that provides a detailed log of system, security, and application events on your computer.

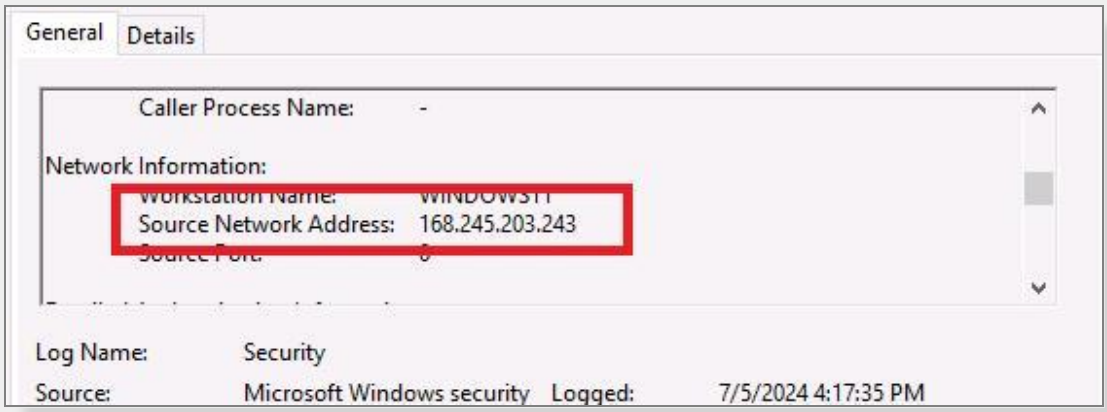
It collects data from Windows logs and categorizes them into different types such as Information, Warning, Error, Success Audit, and Failure Audit. This tool is particularly useful for troubleshooting hardware and software issues, as it records significant occurrences in the operating system and other programs. By analyzing the logs in the Event Viewer, users or administrators can identify patterns that may indicate potential problems. However, interpreting the data requires some technical knowledge and understanding of Windows processes.

- Using Event properties, locate the source network address of an attacker.

Expand this hint for guidance on locating the Source Network Address by using Event properties.

- Select any of the logs with an Event ID of **4625**, and then double-click the log name.

- On the Event Properties page, scroll down, and then in Network Information, locate the **Source Network Address**.



Want to learn more? Review the documentation on locating the Source Network Address by using Event properties.

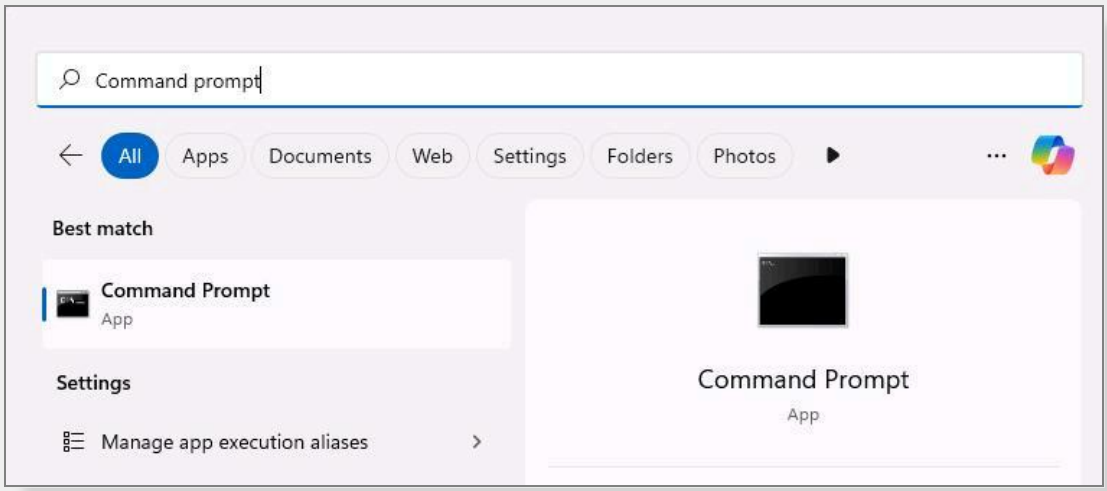
Locating the Source Network Address by using Event Properties involves navigating through the Windows Event Viewer.

When a network-related event occurs, it's logged in the Event Viewer with details including the Source Network Address. To find this, you open the Event Viewer, go to the relevant log (like 'Security'), and find the event of interest. Upon selecting the event, the 'Event Properties' window will open, displaying detailed information about the event, including the 'Source Network Address'. This address indicates the origin of the network traffic related to the event, which can be crucial for network troubleshooting and security investigations.

- Use a command prompt to PING the SentinelHexelo-VM virtual machine.

Expand this hint for guidance on using the PING command.

- On the **Windows 11** desktop, select the Search icon, and then enter T Command Prompt.



- In the Command Prompt console, enter T ping, followed by the SentinelHexelo-VM Public IP address, followed by T -t, and then select **Enter**.

Want to learn more? Review the documentation on using the PING command.

The PING command is a network diagnostic tool used to test the reachability of a host on an Internet Protocol (IP) network.

It operates by sending Internet Control Message Protocol (ICMP) Echo Request messages to the target host and waiting for an Echo Reply. The time taken for these messages to be sent and received is measured and reported, providing valuable information about network latency and packet loss. This command is widely used for troubleshooting network connectivity issues. It's important to note that some hosts may not respond to ICMP Echo Requests due to firewall settings or other security measures.

Check your work

Verify

Visualize the attacks on a map.

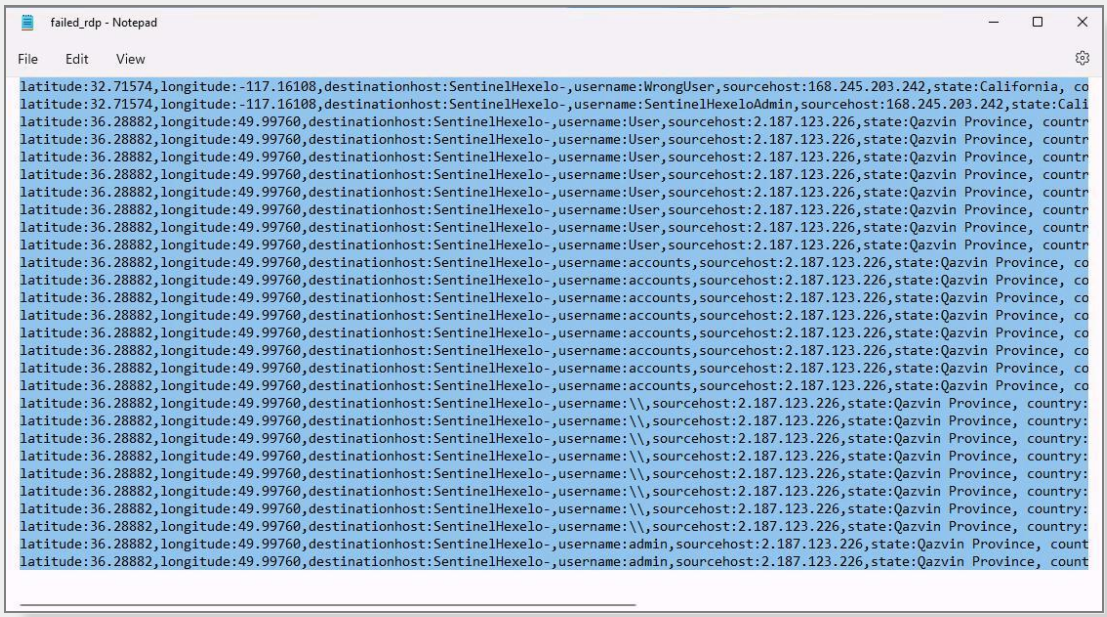
Hints Enabled

No Yes

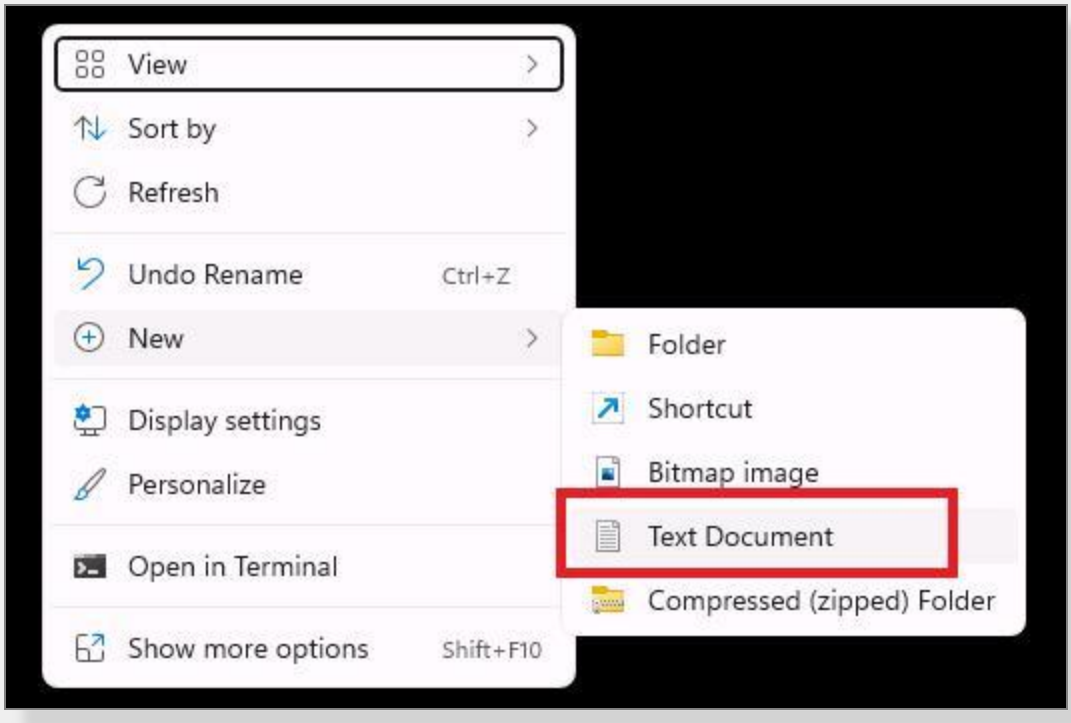
- By using the **Failed_RDP.log**, create a new custom MMA-based log named T Failed-RDP.txt.

Expand this hint for guidance on creating a new custom MMA-based log.

- In the **SentinelHexelo-VM** virtual machine, open the **Failed_RDP.log** log file, select all of the records, and then select **Ctrl+A**.



- Minimize the SentinelHexelo-VM virtual machine, right-click the **Windows 11** desktop, and select **New | Text document**.



- Paste the copied Failed_RDP.txt content into the new text document, and then save it as Failed-RDP.txt.

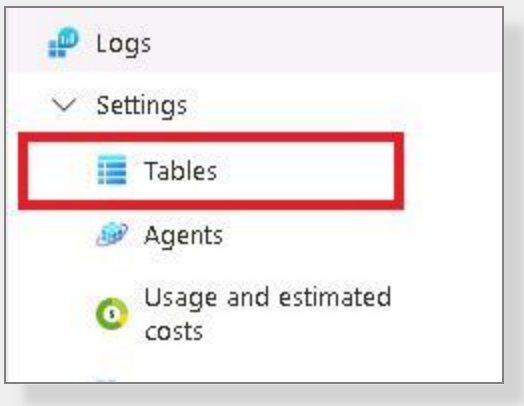
- Save and close **Failed-RDP.txt**.

Want to learn more? Review the documentation on creating a new custom MMA-based log.

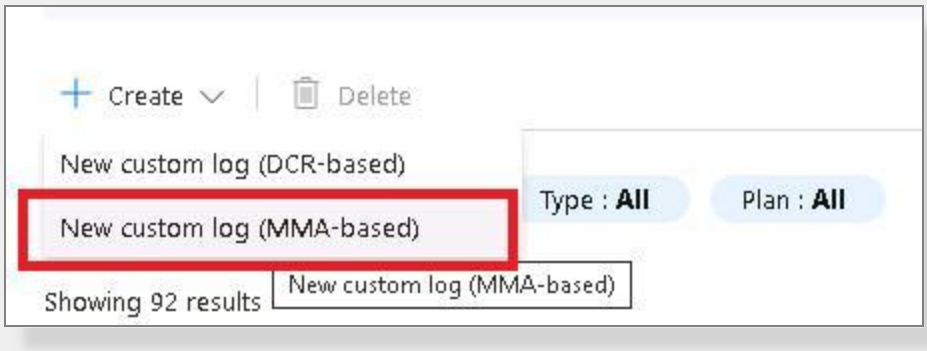
- By using the **Failed-RDP.txt** file and a path of T C:\Programdata\failed_rdp.log, create a custom log named T FAILED_RDP_GEO.

Expand this hint for guidance on creating a custom log.

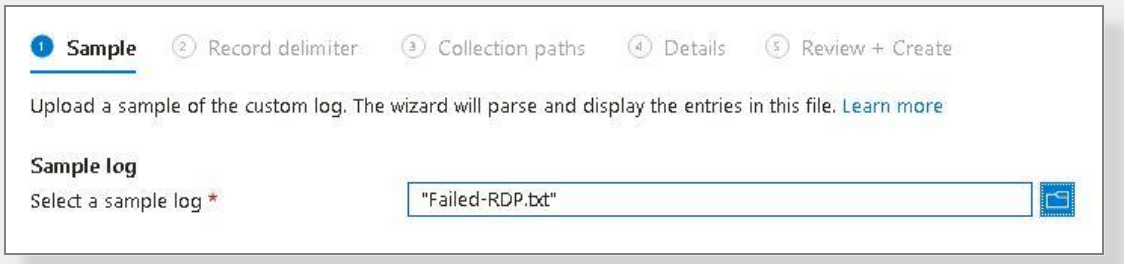
- In Search resources, services, and docs (G+/), search for and select Log Analytics Workspaces, and then select the **SentinelHexelo-LAW** workspace.
- On the SentinelHexelo-LAW workspace Overview page, in Settings, select **Tables**.



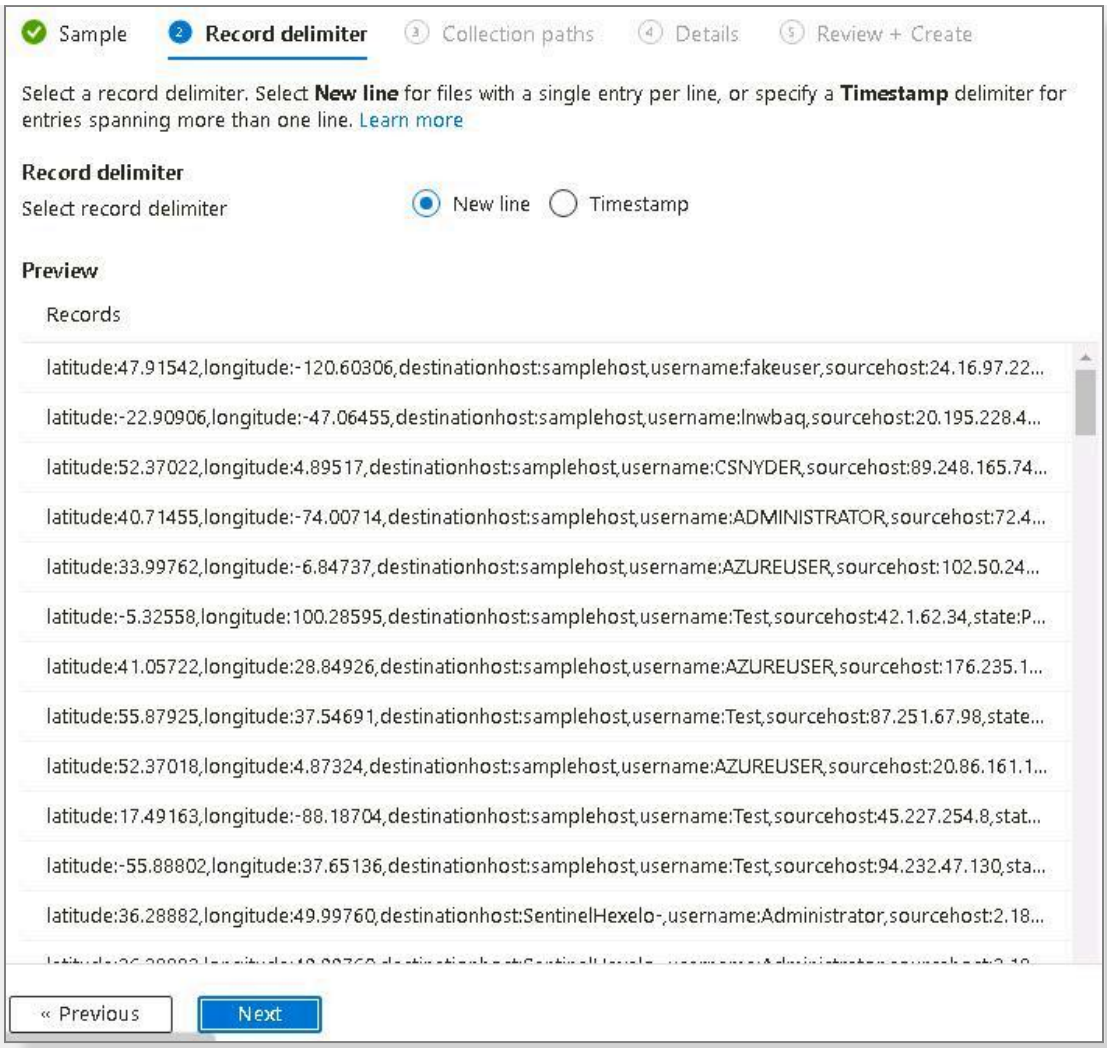
- On the SentinelHexelo-LAW | Tables** page, select **Create**, and then select **New custom log (MMA-based)**.



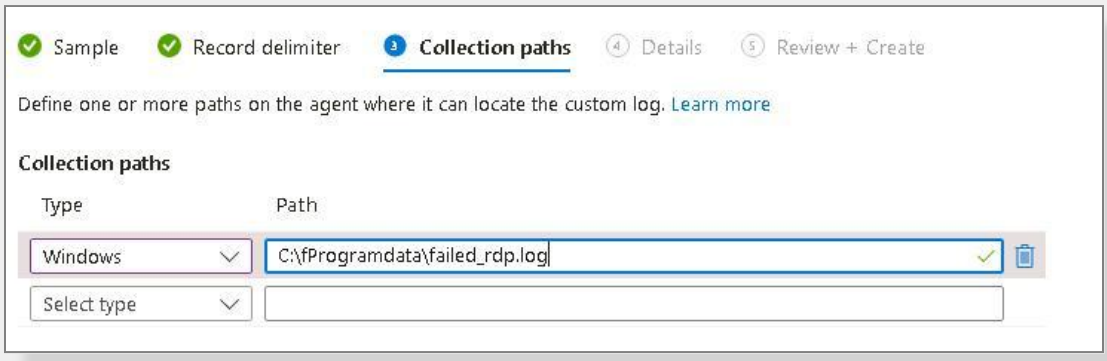
- On the Create a custom log page, on the Sample tab, in Sample log, by using the Select a file icon, search for and select the **Failed-RDP.txt** file, and then select **Next**.



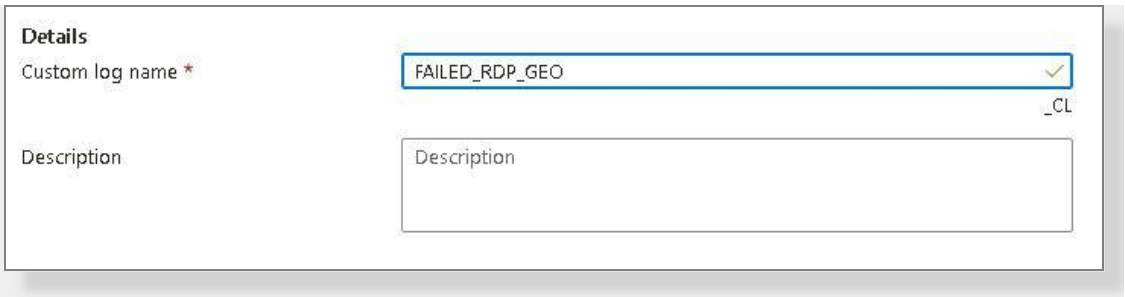
- On the Record delimiter tab, review the records, and then select **Next**.



- On the Collection paths page, in Collection paths, in Type, select **Windows**, and then in Path, enter T C:\Programdata\failed_rdp.log.



- Select **Next**, and then on the Details tab, in Custom log name, enter T FAILED_RDP_GEO, and then select **Next**.



- On the Review + Create tab, review the details, and then select **Create**.

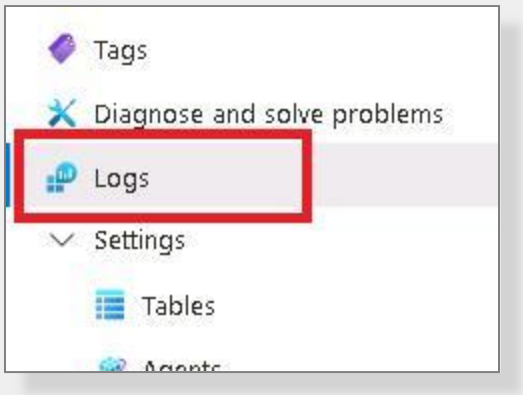
Creating a new custom Microsoft Monitoring Agent (MMA)-based log in Azure Sentinel involves a few steps.

First, you need to install the MMA agent on the machine from which you want to collect logs. Then, you configure the agent to collect custom logs by creating a configuration file that specifies the log file paths and other parameters. This configuration file is then imported into the MMA agent. Once the agent starts collecting the custom logs, you can connect it to Azure Sentinel. In Azure Sentinel, you create a new custom log table where the logs will be stored and analyzed.

- Run the T FAILED_RDP_GEO_CL query.

Expand this hint for guidance on threat hunting.

- On the SentinelHexelo-LAW | Tables page, select **Logs**, and then close any open windows.

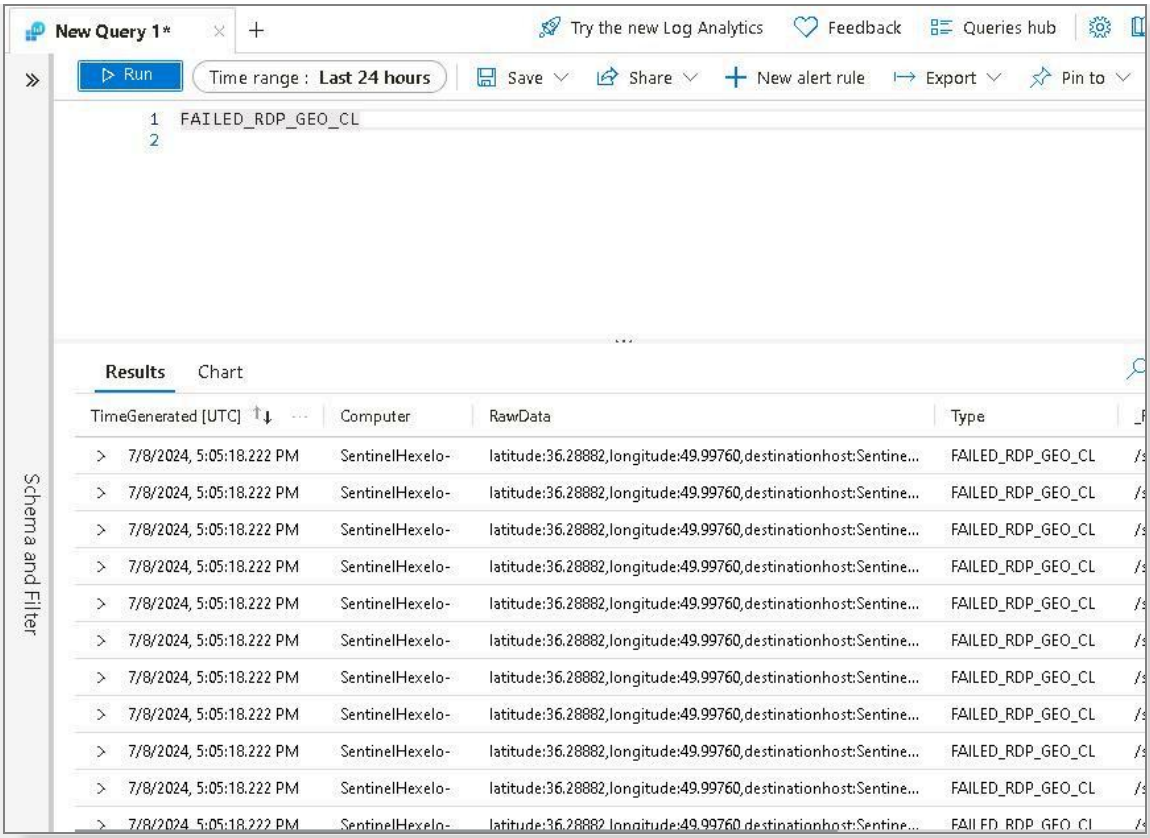


>

- On the Logs page, in New Query 1, enter FAILED_RDP_GEO_CL, and then select **Run**.

Want to learn more? Review the documentation on threat hunting.

Your screen should look like the following:



Running a query in Azure Sentinel involves using the Kusto Query Language (KQL) to retrieve, filter, or analyze data. You start by navigating to the 'Log Analytics' workspace, where you can input your query into the query editor. The query can be as simple as retrieving all records from a specific table, or more complex involving joins, filters, and aggregations. Once the query is written, you execute it by clicking 'Run', and the results are displayed in the results pane. These results can be used for further analysis, creating visualizations, or triggering alerts based on specific conditions.

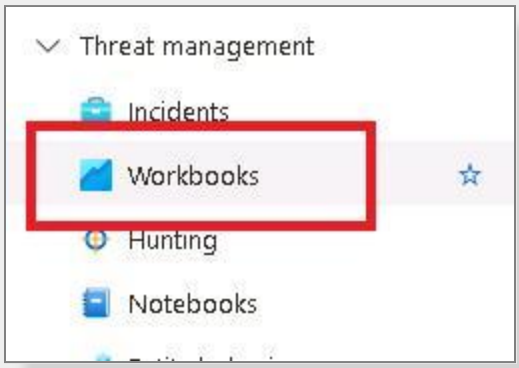
- Create a Workbook by using the following query:

```
FAILED_RDP_GEO_CL
|extend username = extract(@"username:([^,]+)", 1, RawData),
timestamp = extract(@"timestamp:([^,]+)", 1, RawData),
latitude = extract(@"latitude:([^,]+)", 1, RawData),
longitude = extract(@"longitude:([^,]+)", 1, RawData),
sourcehost = extract(@"sourcehost:([^,]+)", 1, RawData),
state = extract(@"state:([^,]+)", 1, RawData),
label = extract(@"label:([^,]+)", 1, RawData),
destination = extract(@"destinationhost:([^,]+)", 1, RawData),
country = extract(@"country:([^,]+)", 1, RawData)
|where destination != "samplehost"
|where sourcehost != ""
|summarize event_count=count() by timestamp, label, country, state, sourc
```

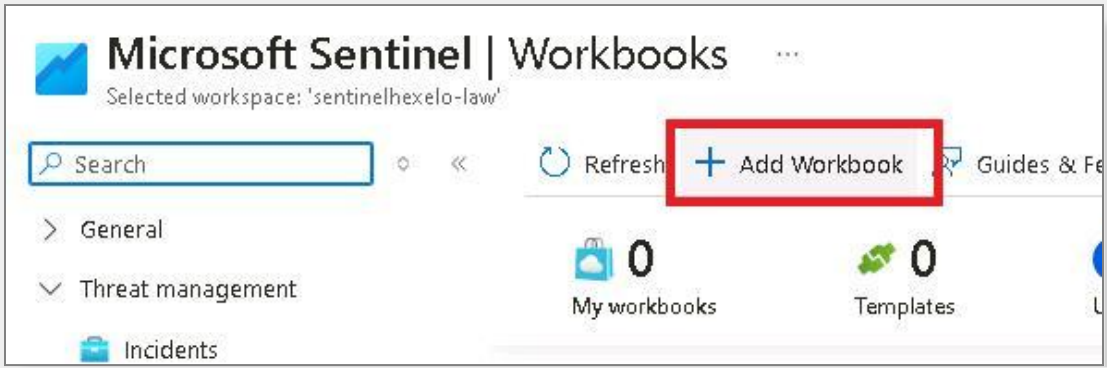
Expand this hint for guidance on creating a workbook.

- On the **Windows 11**, return to the Microsoft Setinel | Overview page, and then in Search resources, services, and docs (G+/), search for and select Microsoft Sentinel.
- On the Microsoft Sentinel | Overview page, review the Failed_RDP_GEO_CL hits.

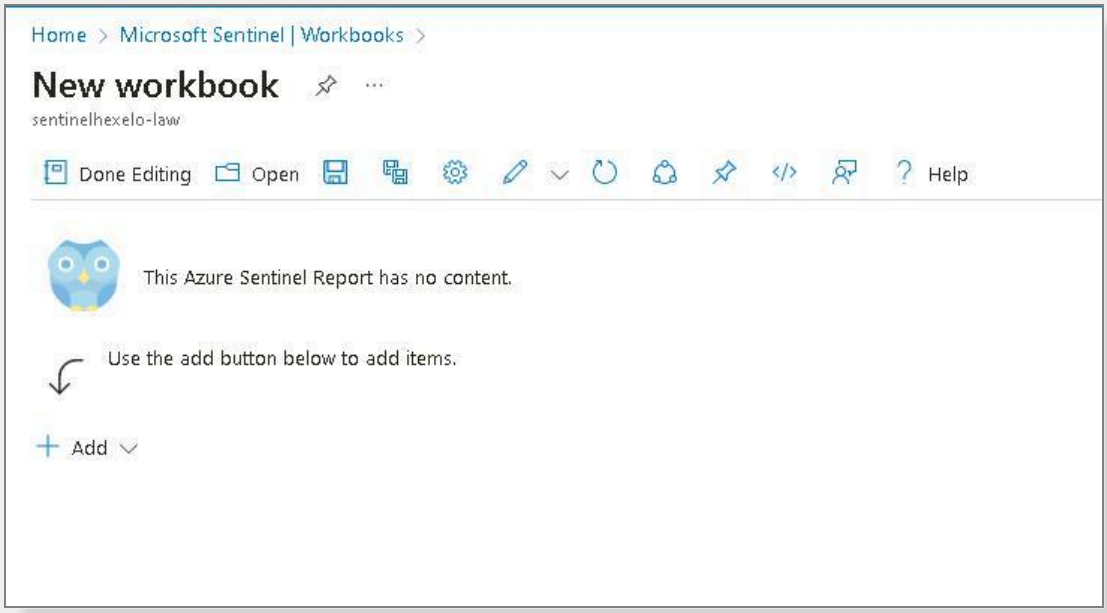
- In Threat management, select **Workbooks**.



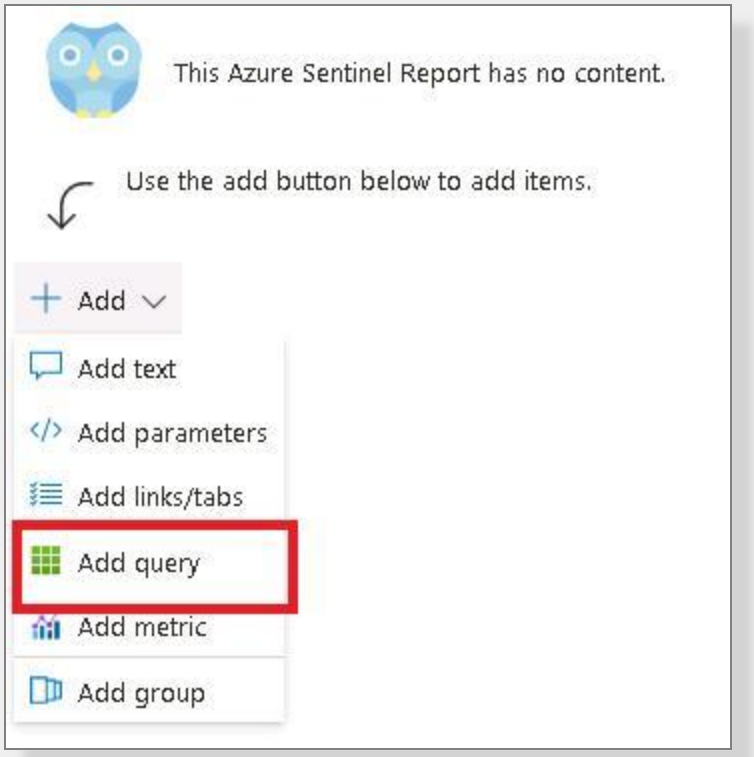
- On the Microsoft Sentinel | Workbooks page, select **Add workbook**.



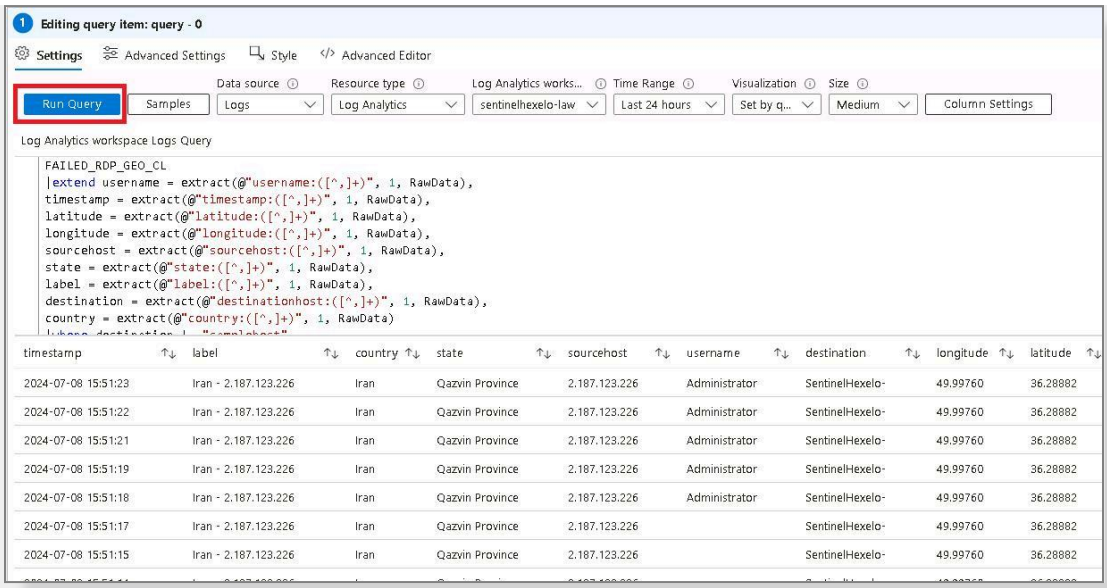
- On the New workbook page, select **Edit**, and then remove any queries.



- Select **+ Add**, and then select **Add query**.



- Insert the above supplied query, and then select **Run query**.



Want to learn more? Review the documentation on creating a workbook.

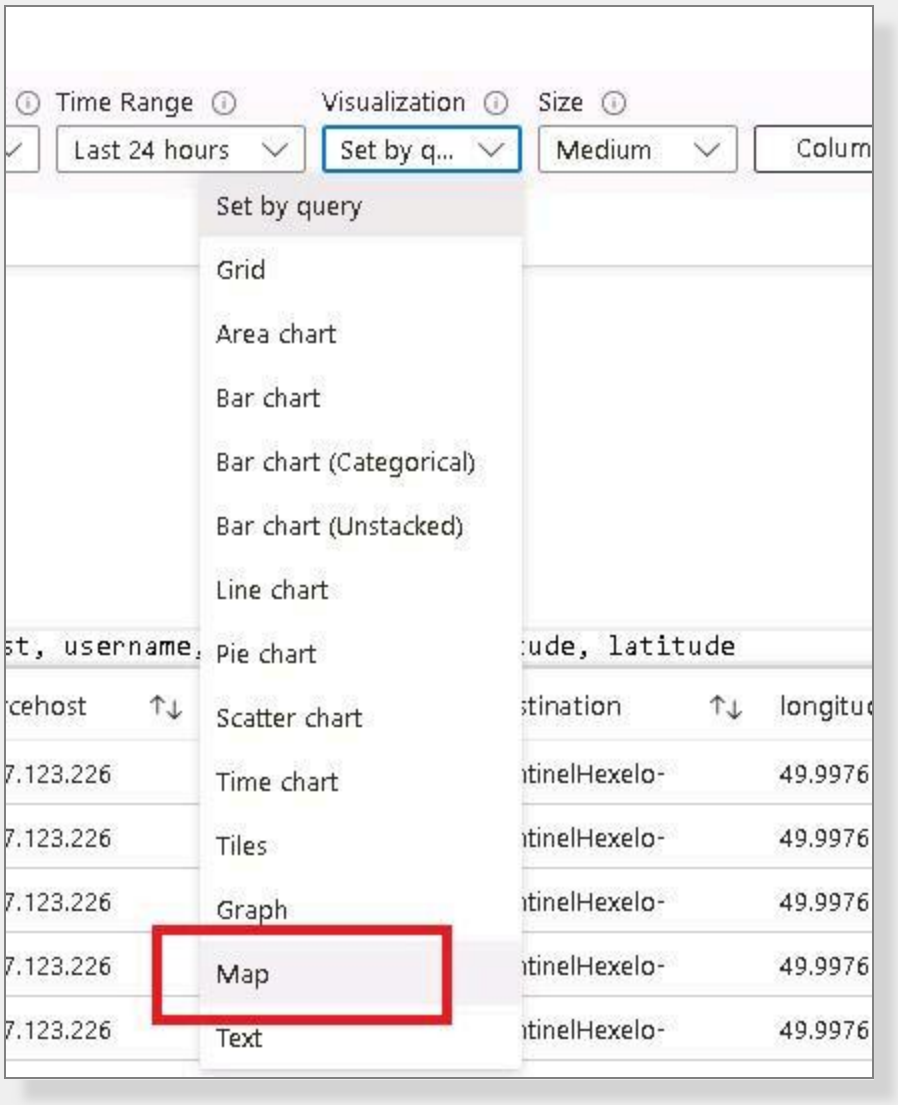
Creating a workbook in Azure Sentinel is a process that allows you to visualize and analyze your data in a customizable and shareable format.

You start by navigating to the 'Workbooks' section in Azure Sentinel and clicking on 'New' to create a new workbook. In the workbook, you can add various types of visualizations such as charts, tables, and graphs, and bind them to data using Kusto Query Language (KQL) queries. The workbook can be saved and shared with others, providing a powerful tool for collaborative analysis. Remember, appropriate permissions in Azure are required to create and modify workbooks.

- Visualize the query as a map.

Expand this hint for guidance on visualizing a query as a map.

- On the New workbook page, select the Visualization dropdown, and then select **Map**.



- On the Map Settings blade, review the settings, and then select **Apply**.

Want to learn more? Review the documentation on visualizing a query as a map.

Visualizing a query as a map in Azure Sentinel involves using the Map visualization feature, which is particularly useful for geographically-oriented data.

You start by running a Kusto Query Language (KQL) query that includes geographical data, such as IP addresses. Azure Sentinel can convert these into geographical coordinates. In the results pane, you select 'Map' as the visualization type. The map will display markers or heatmaps based on the geographical data from your query, providing a visual representation of the geographical distribution of your data. This can be particularly useful for identifying patterns or trends that are related to specific geographical locations.

Check your work

Verify

Summary

Congratulations, you have completed the **Map Cyber Attacks by Using Microsoft Sentinel** Challenge Lab.

You have accomplished the following:

- Added Microsoft Sentinel to a workspace.
- Created a new virtual machine.
- Created a Network security group.
- Enabled the Microsoft Defender plan.
- Connected a workspace to a virtual machine.
- Opened a VM by using Remote Desktop Connection.
- Disabled Windows Defender Firewall on the virtual machine.
- Replaced API keys by using Windows Powershell ISE.
- PINGed a virtual machine.
- Created a new custom MMA-based log named.
- Created a custom log.
- Created a new workbook.
- Visualized a query as a map.

Your feedback is important!

As you end your Challenge Lab, please take a few minutes to complete the short survey that will appear in the next window.

Alternatively, you may provide your feedback directly to Challenge Labs feedback.

Be sure to check out the other Challenge Labs in this series:

- Create detections and perform investigations by using Microsoft Sentinel [Guided]
- Importing Splunk data into Microsoft Sentinel [Guided]
- Introduction to Microsoft Sentinel, Azure Monitoring agent, and syslog incident monitoring [Guided]
- Explore Microsoft Sentinel [Guided]