

Creating a Honeypot with Azure and Microsoft Sentinel

1. Create the Resource Group

Create a resource group ...

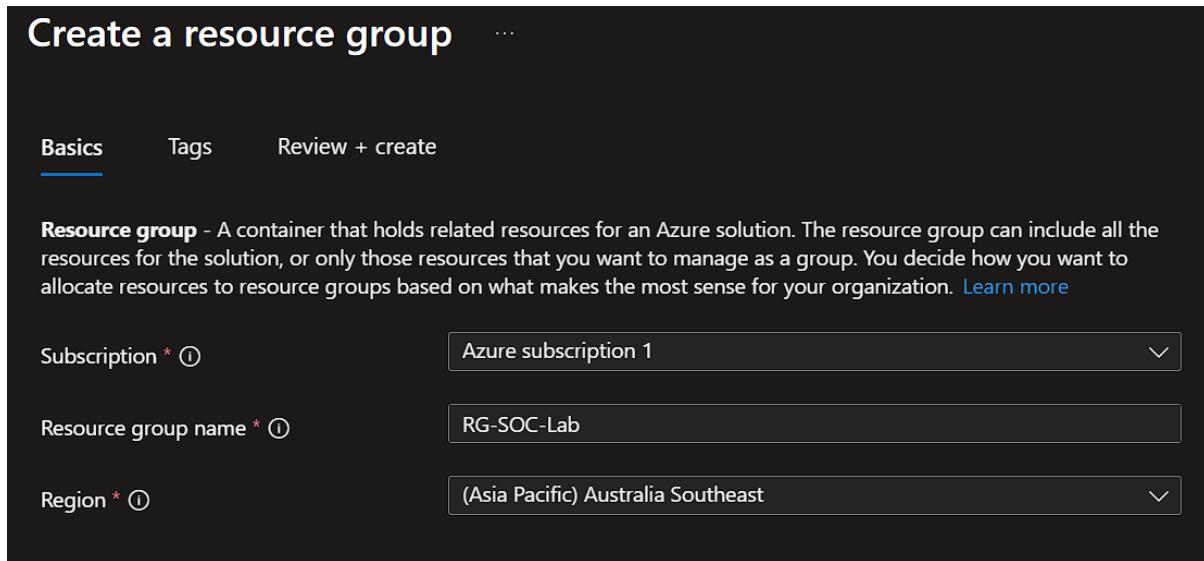
Basics Tags Review + create

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

Subscription * ⓘ Azure subscription 1

Resource group name * ⓘ RG-SOC-Lab

Region * ⓘ (Asia Pacific) Australia Southeast



You need an active Azure subscription. After subscribing, create a resource group in your preferred region and give it a distinctive name for easy identification — for example: **RG-SOC-Lab**.

2. Create the Virtual Network

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 *

Resource group *
[Create new](#)

Instance details

Virtual network name *

Region *
[Deploy to an Azure Extended Zone](#)

Subnets	IP address range	Size	NAT gateway
default	10.0.0.0 - 10.0.0.255	/24 (256 addresses)	-

The Resource Group and Virtual Machine must be internet-connected. First, set up a virtual network to create the subnet the VM will reside on. Use the default settings and name the virtual network **VNet-SOC-Lab**.

Create virtual network ...

⌚ Deploying...

Basics Security IP addresses Tags **Review + create**

[View automation template](#)

Basics

Subscription	Azure subscription 1
Resource Group	RG-SOC-Lab
Name	VNet-SOC-Lab
Region	Australia Southeast

Security

Azure Bastion	Disabled
Azure Firewall	Disabled
Azure DDoS Network Protection	Disabled

IP addresses

Address space	10.0.0.0/16 (65,536 addresses)
Subnet	default (10.0.0.0/24) (256 addresses)

Tags

3. Create the Virtual Machine

Labuser:cyberlab123!

Create a Windows 10 Enterprise virtual machine and assign it an inconspicuous name (for example, **CORP-NET-AU-1**) so it doesn't appear to be a honeypot. After exposing the VM to the internet it may receive connections quickly—often within minutes. Provide a simple username and password and ensure the VM is deployed to the same virtual network you

created earlier.

Create a virtual machine



Help me create a VM optimized for high availability

Help me create a low cost VM

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

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

Subscription * ⓘ

Azure subscription 1

Resource group * ⓘ

RG-SOC-Lab

[Create new](#)

Instance details

Virtual machine name * ⓘ

CORP-NET-AU-1

Region * ⓘ

(Asia Pacific) Australia Southeast

[Deploy to an Azure Extended Zone](#)

Availability options ⓘ

No infrastructure redundancy required

Security type ⓘ

Trusted launch virtual machines

[Configure security features](#)

Image * ⓘ

Windows 10 Enterprise, version 22H2 - x64 Gen2

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

VM architecture ⓘ

Arm64

x64

i Arm64 is not supported with the selected image.

Run with Azure Spot discount ⓘ



Size * ⓘ

Standard_D2s_v3 - 2 vcpus, 8 GiB memory (US\$91.25)

[See all sizes](#)

Enable Hibernation ⓘ



i Hibernate is not supported by the size that you have selected. Choose a size that is compatible with Hibernate to enable this feature. [Learn more](#)

Administrator account

Username * ⓘ

labuser

Password *

Confirm password *

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ

None

[< Previous](#)

[Next : Disks >](#)

[Review + create](#)

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ

- None
- Allow selected ports

Select inbound ports *

RDP (3389)



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

Licensing

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

Create a virtual machine

[Help me create a VM optimized for high availability](#)[Help me create a low cost 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

VNet-SOC-Lab (RG-SOC-Lab)

[Edit virtual network](#)

Subnet *

(New) snet-australiasoutheast-1

[Edit subnet](#)

10.0.1.0 - 10.0.1.255 (256 addresses)

Public IP

(new) CORP-NET-AU-1-ip

[Create new](#)

Public IP addresses have a nominal charge. [Estimate price](#)

NIC network security group

None

Basic

Advanced

Public inbound ports *

None

Allow selected ports

Select inbound ports *

RDP (3389)



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

Delete public IP and NIC when VM is deleted



Enable accelerated networking



Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Load balancing options

None

Azure load balancer

Supports all TCP/UDP network traffic, port-forwarding, and outbound flows.

Application gateway

Web traffic load balancer for HTTP/HTTPS with URL-based routing, SSL termination, session persistence, and web application firewall.

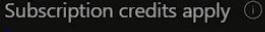
Create a virtual machine

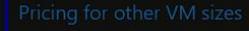
...  Help me create a VM optimized for high availability  Help me create a low cost VM

i Running final validation...

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

Price

1 X Standard D2s v3
by Microsoft 
[Terms of use](#) | [Privacy policy](#)

0.1250 USD/hr 

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

! You have set RDP port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.

Basics

Subscription	Azure subscription 1
Resource group	RG-SOC-Lab
Virtual machine name	CORP-NET-AU-1
Region	Australia Southeast
Availability options	No infrastructure redundancy required
Zone options	Self-selected zone
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable vTPM	Yes
Integrity monitoring	No
Image	Windows 10 Enterprise, version 22H2 - Gen2
VM architecture	x64
Size	Standard D2s v3 (2 vcpus, 8 GiB memory)
Enable Hibernation	No
Username	labuser
Public inbound ports	RDP
Already have a Windows license?	Yes
License type	Windows Client
Azure Spot	No

Disks

OS disk size	Image default
OS disk type	Premium SSD LRS
Use managed disks	Yes

RG-SOC-Lab - Resource group

Subscription (more) : Azure subscription 1
Subscription ID : ed5ca18-089-478-8029-2af05e06311
Tags (edit) : Add tags

Resources Recommendations

Name	Type	Location
CORP-NET-AU-1	Virtual machine	Australia Southeast
CORP-NET-AU-1-nsg	Public IP address	Australia Southeast
CORP-NET-AU-1-nsg	Network security group	Australia Southeast
corp.net.au-176	Network Interface	Australia Southeast
CORP-NET-AU-1-1-DataDisk_1-c42745332c94ec197899f83d85d04ef	Disk	Australia Southeast
VNet-SOC-Lab	Virtual network	Australia Southeast

4. Expose VM to the Internet

Create an inbound rule that exposes the VM to the internet by replacing the default rules with a permissive custom rule that allows all traffic. This is intentionally unsafe and should never be used in production; it's for a honeypot environment only. Name the rule **DANGER_AllowAnyCustomAnyInbound**.

CORP-NET-AU-1-nsg

Inbound security rules (1 inbound, 0 outbound)

Priority	Name	Port	Protocol	Source	Destination	Action
300	AllowInbound	Any	Any	Any	Any	Allow
65000	AllowCustomInbound	Any	Any	Any	Any	Allow
65000	DenyInbound	Any	Any	Any	Any	Deny
65000	AllowOutbound	Any	Any	VirtualNetwork	Internet	Allow
65000	AllowCustomOutbound	Any	Any	Any	Any	Allow
65000	DenyOutbound	Any	Any	Any	Any	Deny

CORP-NET-AU-1-nsg | Inbound security rules ☆ ...

Network security group

Search Search icon Filter icon Add Hide default rules Refresh Delete

Network security group security rules are evaluated by priority

Filter by name Search icon Port Sort icon

Priority ↑↓

Priority	Action
65000	<input type="checkbox"/>
65001	<input type="checkbox"/>
65500	<input type="checkbox"/>

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

The screenshot shows the Azure portal interface for managing Network Security Group (NSG) inbound security rules. The main title is "CORP-NET-AU-1-nsg | Inbound security rules". Below it, it says "Network security group". The top navigation bar includes a search bar, a filter icon, an "Add" button, a "Hide default rules" link, a "Refresh" button, and a "Delete" button. A message states "Network security group security rules are evaluated by priority". To the right is a "Filter by name" search bar and a "Port" dropdown menu. The main content area lists three security rules with their priorities: 65000, 65001, and 65500. Each rule has a checkbox next to its priority value. On the left side, there is a sidebar with various options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Settings (expanded to show Inbound security rules, Outbound security rules, Network interfaces, Subnets, Properties, and Locks), and Inbound security rules (which is currently selected). The "Inbound security rules" option is highlighted with a blue background.

Add inbound security rule

CORP-NET-AU-1-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 *

DANGER_AllowAnyCustomAnyInbound

Description

⚠ MS SQL DB port 1433 is exposed to the Internet. We do not recommend exposing database ports to the Internet and suggest only exposing them to your front-end tier inside your virtual network.

⚠ Oracle DB port 1521 is exposed to the Internet. We do not recommend exposing database ports to the Internet and suggest only exposing them to your front-end tier inside your virtual network.

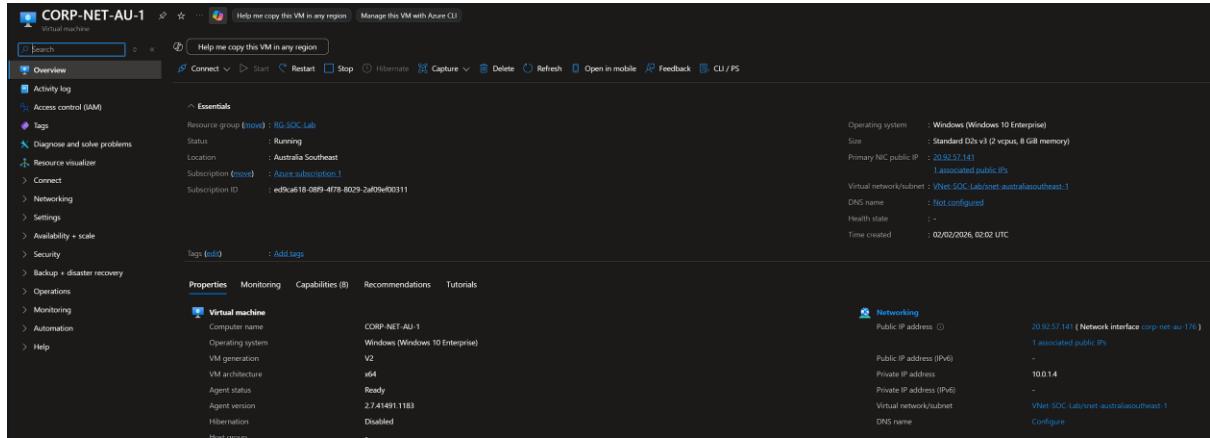
⚠ Mysql DB port 3306 is exposed to the Internet. We do not recommend exposing database ports to the Internet and suggest only exposing them to your front-end tier inside your virtual network.

⚠ Postgres DB port 5432 is exposed to the Internet. We do not recommend exposing database ports to the Internet and suggest only exposing them to your front-end tier inside your virtual network.

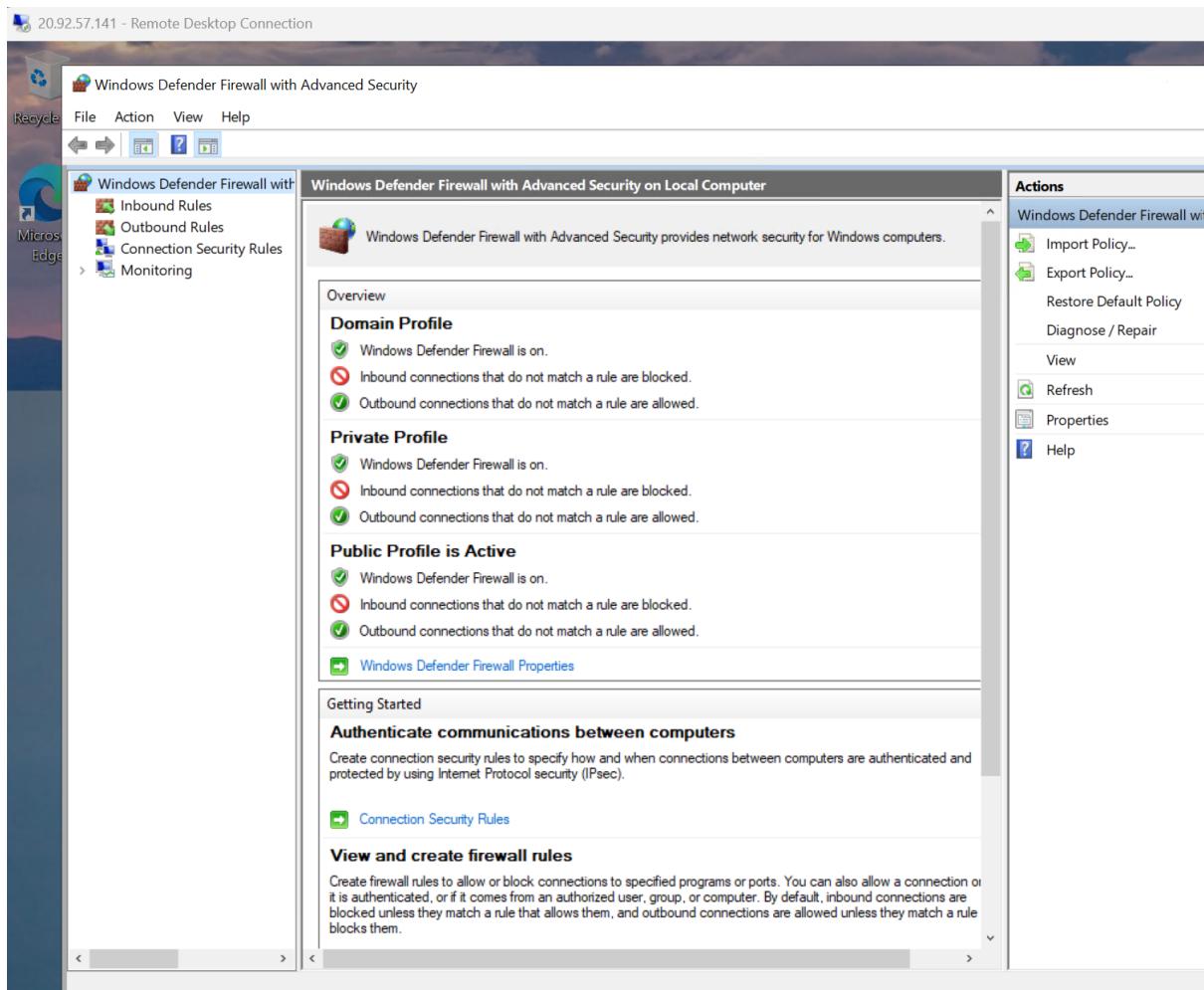
Add Cancel Give feedback

5. Remote into VM and Disable Firewall

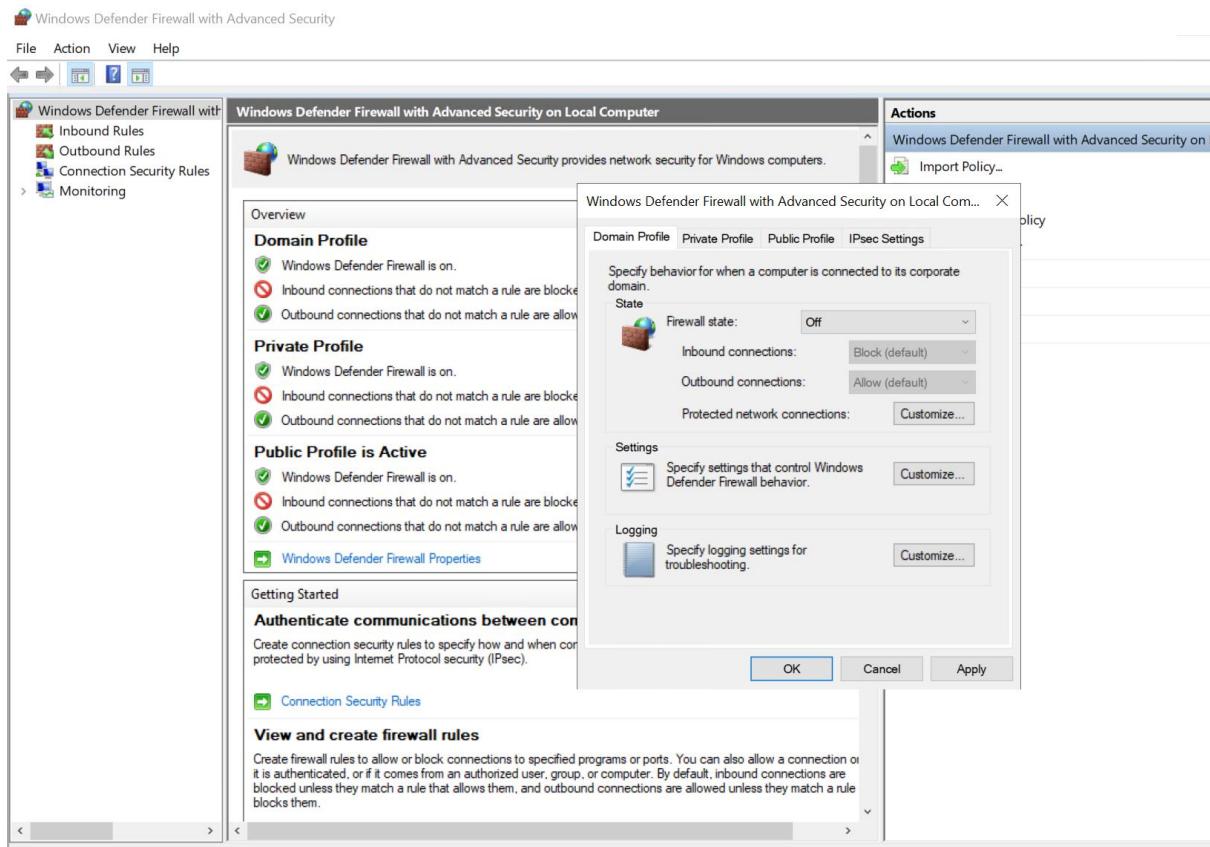
Obtain the VM's public IP and RDP into it using the credentials you created. Once connected, disable the firewall completely to leave the machine exposed to all incoming traffic.



The screenshot shows the Azure portal interface for a virtual machine named 'CORP-NET-AU-1'. The 'Overview' tab is selected, displaying basic information such as Resource group (RG SOC Lab), Status (Running), Location (Australia Southeast), and Subscription (Azure subscription). It also shows the operating system (Windows 10 Enterprise), size (Standard D2s v3 (2 vcpus, 8 GiB memory)), and creation time (02/02/2026, 02:02 UTC). The 'Networking' section shows a public IP address (20.92.57.141) and a private IP address (10.0.1.4).



The screenshot shows the Windows Defender Firewall with Advanced Security interface. The 'Inbound Rules' section is visible on the left, while the main pane displays the 'Windows Defender Firewall with Advanced Security on Local Computer' overview. It highlights that the Domain Profile has inbound connections blocked and outbound connections allowed. The Private Profile also has inbound connections blocked and outbound connections allowed. The Public Profile is active. The interface includes sections for 'Getting Started' (Authenticate communications between computers) and 'View and create firewall rules' (Create firewall rules to allow or block connections to specified programs or ports). On the right, there is an 'Actions' sidebar with options like Import Policy, Export Policy, Restore Default Policy, Diagnose / Repair, View, Refresh, Properties, and Help.



6. Creating the Log Analytics Workspace

Create a Log Analytics workspace and connect it to the VM so it forwards events. Name the workspace **LAW-SOC-Lab-0000** for easy identification.

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](#) X

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 * ⓘ RG-SOC-Lab Create new

Instance details

Name * ⓘ LAW-SOC-Lab-0000 ✓

Region * ⓘ Australia Southeast ▼

7. Linking Microsoft Sentinel

Proceed to link Microsoft Sentinel to the Log Analytics Workspace.

Home > Microsoft Sentinel > 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.

New Microsoft Sentinel workspaces created by authorized users are automatically onboarded and redirected to the Defender portal. [Learn more](#)

Enter workspace name	Location	ResourceGroup	Subscription	Directory
LAW-SOC-Lab-0000	Australia Southeast	RG-SOC-Lab	Azure subscription 1	Home

... Adding Microsoft Sentinel X

Adding Microsoft Sentinel to workspace 'LAW-SOC-Lab-0000'

8. Connect VM to Log Analytics Workspace

Connect the VM to the Log Analytics workspace (Sentinel enabled). In Microsoft Sentinel, install the **Windows Security Events** solution to simplify event parsing. Configure Windows Security Events using the Azure Monitor Agent (the legacy method is deprecated). Create a

Security Event data collection rule, link it to the Windows VM, and verify the agent/extension appears on the VM.

The screenshot shows the Microsoft Sentinel Content hub interface. At the top, there are navigation links: Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel. Below the header, it says "Selected workspace: 'law-soc-lab-0000'". The main area has a sidebar with categories: General, Threat management, Content management (which is expanded to show Content hub, Repositories, and Community), Configuration, and SIEM Migration. The Content hub section is currently selected. It displays statistics: 456 Solutions, 324 Standalone contents, 0 Installed, and 0 Updates. A search bar at the top right shows the query "security event". Below the search bar, there is a message: "Didn't find what you were looking for? We're showing a limited set of results. Try refining your search for more specific results." A table lists search results:

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



Windows Security Events

»

Microsoft
Provider

Microsoft
Support

3.0.10
Version

Description

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

- Review the solution [Release Notes](#)

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

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

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

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

[Learn more about Microsoft Sentinel](#) | [Learn more about Solutions](#)

Content type ⓘ

20
Analytics rule

2
Data connector

50
Hunting query

2
Workbook

Category ⓘ

Security - Threat Protection

Pricing ⓘ

Free

Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel | Content hub >

Windows Security Events

74 Installed content items 22 Configuration needed

Windows Security Events

Microsoft Provider | Microsoft Support | Version 3.0.10

Description

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

- Review the solution [Release Notes](#)

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

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

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

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

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

Learn more about Microsoft Sentinel | Learn more about Solutions

Content type: 20 Analytics rule, 2 Data connector, 50 Hunting query

Workbook: 2

Category: ① Security - Threat Protection

Pricing: ① Free

Content name	Created content	Content type	Version	Status
Security Events via Legacy Agent	1 items	Data connector	1.0.0	Installed
Windows Security Events via AMA	1 items	Data connector	1.0.0	Installed
AD FS Remote Auth Sync Connection	--	Analytics rule	1.0.4	Installed
AD FS Remote HTTP Network Connection	--	Analytics rule	1.0.2	Installed
AD user enabled and password not set within 48 hours	--	Analytics rule	1.0.4	Installed
ADFS Database Named Pipe Connection	--	Analytics rule	1.0.2	Installed
Excessive Windows Logon Failures	--	Analytics rule	2.0.3	Installed
Exchange QAB Virtual Directory Attribute Containing Potential Webshell	--	Analytics rule	1.0.4	Installed
Gain Code Execution on ADFS Server via SMB + Remote Service or Scheduled Task	--	Analytics rule	1.2.1	Installed
Microsoft Entra ID Local Device Join Information and Transport Key Registry Keys Access	--	Analytics rule	1.0.5	Installed
New EXE deployed via Default Domain or Default Domain Controller Policies	--	Analytics rule	1.0.2	Installed
Non Domain Controller Active Directory Replication	--	Analytics rule	1.0.5	Installed
NRT Base64 Encoded Windows Process Command-lines	--	Analytics rule	1.0.2	Installed
NRT Process executed from binary hidden in Base64 encoded file	--	Analytics rule	1.0.2	Installed
NRT Security Event log cleared	--	Analytics rule	1.0.1	Installed
Potential Fodhelper UAC Bypass	--	Analytics rule	1.0.2	Installed
Potential re-named sdelete usage	--	Analytics rule	1.0.3	Installed
Process Execution Frequency Anomaly	--	Analytics rule	1.0.6	Installed
Scheduled Task Hide	--	Analytics rule	1.0.1	Installed
Sdelete deployed via GPO and run recursively	--	Analytics rule	1.0.2	Installed
SecurityEvent - Multiple authentication failures followed by a success	--	Analytics rule	1.0.7	Installed
Starting or Stopping HealthService to Avoid Detection	--	Analytics rule	1.0.2	Installed
AD Account Lockout	--	Hunting query	1.0.0	Installed
Commands executed by WMI on new hosts - potential Impacket	--	Hunting query	2.0.2	Installed
Crash dump disabled on host	--	Hunting query	2.0.1	Installed
Script script daily summary breakdown	--	Hunting query	2.0.1	Installed
Decoy User Account Authentication Attempt	--	Hunting query	2.0.2	Installed
Discord download invoked from cmd line	--	Hunting query	2.0.1	Installed
Domain controller installation media creation	--	Hunting query	1.0.1	Installed

Windows Security Events via AMA 1 items Data connector 1.0.0 Installed

 Windows Security Events via AMA

»

Disconnected Status	 Microsoft Provider	 -- Last Log Received
---------------------	--	--

Description

You can stream all security events from the Windows machines connected to your Microsoft Sentinel workspace using the Windows agent. This connection enables you to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities. For more information, see the [Microsoft Sentinel documentation](#).

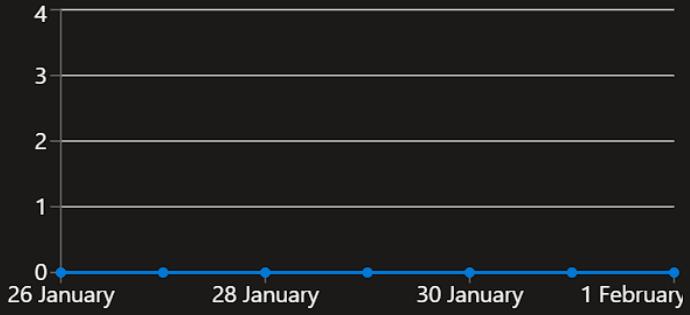
Last data received

--

Content source  Version
Windows Security Events 1.0.0

Author Supported by
Microsoft [Microsoft Corporation](#) | [Email](#)

Data received [Go to query](#)



The chart displays a single data series named "SecurityEvents". The Y-axis represents the count of events, ranging from 0 to 4. The X-axis shows dates from 26 January to 1 February. Four data points are plotted at (26 Jan, 0), (27 Jan, 0), (28 Jan, 0), (29 Jan, 0), (30 Jan, 0), and (1 Feb, 0). A vertical blue bar is positioned at the value 0.

0

Data types

 SecurityEvents --

[Open connector page](#)

Windows Security Events via AMA

Windows Security Events via AMA

Disconnected Status	Microsoft Provider	Last Log Received
---------------------	--------------------	-------------------

Description

You can stream all security events from the Windows machines connected to your Microsoft Sentinel workspace using the Windows agent. This connection enables you to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities.

Last data received

--

Content source ① Version

Windows Security Events 1.0.0

Author Supported by

Microsoft Microsoft Corporation | Email

Related content

0 Workbooks 1 Queries 20 Analytics rules/templates

Data received

Go to log analytics

0 SecurityEvents

Data types

SecurityEvents --

Prerequisites

To integrate with Windows Security Events via AMA make sure you have:

- ✓ **Workspace data sources:** read and write permissions.
- ⓘ To collect data from non-Azure VMs, they must have Azure Arc installed and enabled. [Learn more](#)

Configuration

Enable data collection rule

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

Refresh ①

Rule name	Created by	Filter name
No results		

+Create data collection rule

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 * DCR-Windows

Subscription * Azure subscription 1

Resource group * RG-SOC-Lab

Create Data Collection Rule

Data collection rule management

Basic Resources Collect Review + create

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

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

Subscriptions	Resource Groups	Resource Types	Locations
Selected: All	Selected: All	Selected: All	Selected: All
<input type="text"/> Search to filter items...		Show Selected	
Scope	Resource Type	Location	
<input checked="" type="checkbox"/> Azure subscription 1			
<input checked="" type="checkbox"/> RG-SOC-Lab			
<input checked="" type="checkbox"/> CORP-NET-AU-1	microsoft.compute/virtualmachines	Australia Southeast	

Create Data Collection Rule

Data collection rule management

Validation passed

Basic Resources Collect Review + create

Basic

Data rule name DCR-Windows

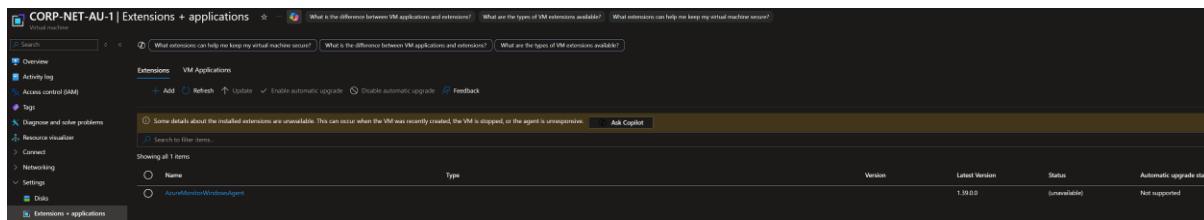
Subscription Azure subscription 1

Resource Group RG-SOC-Lab

Selected resources

Name	Type
corp-net-au-1	microsoft.compute/virtualmachines

Selected events
AllEvents



9. Querying with KQL

Start with basic KQL queries. Initial results show routine activity with no clear signs of compromise. However, after about five minutes—while creating the watchlist—suspicious activity began appearing, indicating probing attempts.

10. Creating the Watchlist

Create a watchlist in Microsoft Sentinel and upload a database file of locations and IPs (for example, MaxMind's GeoIP database). In production, this data would typically come from your provider's backend.

Microsoft Sentinel | Watchlist

Selected workspace: law-soc-lab-0000

Watchlist

0 Watchlists 0 Watchlist Items

My Watchlists Templates (Preview)

Watchlist

What is it?

Microsoft Sentinel watchlist enables the collection of data from external data sources for correlation against the events in your Microsoft Sentinel environment. Once created, leverage watchlists in your search, detection rules, threat hunting, workbooks and response playbooks.

How does it work?

Create a new watchlist by selecting 'Add new' and follow the steps in the new watchlist wizard. You will receive a notification in the notifications area within in the Azure portal that your watchlist was created. Watchlists are stored within your Microsoft Sentinel workspace as name value pairs and are cached for optimal query performance and low latency.

This is what you can do with watchlists

Investigate threats and respond to incidents quickly with fast import of IP addresses, file hashes, etc. from csv files. Then utilize the watchlist name/value pairs for joining and filtering for use in alert rules, threat hunting, workbooks, notebooks and for general queries.

Import business data, such as user lists with privileged system access as a watchlist. Then use the watchlist to create allow and deny lists. For example, use a watchlist that contains a list of terminated employees to detect or prevent them from logging in to the network.

Create allow lists to reduce alert fatigue. For example, use a watchlist to build an allow list to suppress alerts from only a limited set of IP addresses to do specific functions and thus removing benign events from becoming alerts. Use watchlists to enrich your event data with field-value combinations derived from external data sources.

[Learn More](#)

Watchlist wizard

General Source Review + Create

Source type: Local file

File type: CSV file with a header (and)

Number of lines before row with headings: 0

Upload file: geoip-summarized.csv

Drag and drop the file or Browse for file

Search key:

File preview (first 50 rows and first 5 columns)

network	latlon	longlat	cityname	countryname
1.01.0/16	31.494	141.256	-	Australia
1.11.0/16	17.9148	102.336	Ban Chan	Thailand
1.23.0/16	13.8657	102.1917	Nakorn Pathom	Thailand
1.33.0/16	13.8679	102.1951	Nakorn Pathom	Thailand
1.43.0/16	13.8687	102.1979	Bangkok	Thailand
1.53.0/16	13.8659	102.1982	Bangkok	Thailand
1.63.0/16	12.9634	77.855	Bengaluru	India
1.73.0/16	12.9691	77.5902	Bengaluru	India
1.83.0/16	12.9657	77.5945	Bengaluru	India
1.93.0/16	3.1559	101.7468	Alor Setar	Malaysia

Microsoft Sentinel | Watchlist

Selected workspace: law-soc-lab-0000

Watchlist

0 Watchlists 0 Watchlist Items

My Watchlists Templates (Preview)

Search by name, alias and description

Add filter

Name	Alias	Source	Created time	Last updated
geoip	geoip	geoip-summarized.csv	02/02/2026, 14:00:47	02/02/2026, 14:00:47

The screenshot shows the Microsoft Defender Home interface. On the left, there's a navigation sidebar with options like Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel (which is selected), Email & collaboration, and Cloud security. The main area displays 'My Watchlists' with 0 Watchlists and 8K Watchlist Items. It includes a search bar and a table with columns for Name, Alias, Source, Created time, and Last updated. A single entry named 'geopl' is listed.

EventData	EventID
<EventData xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <Data Name="TargetUserName">labuser</Data> <Data Name="TargetDomainName">CORP-NET-A...</Data>	4798
<EventData xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <Data Name="TargetUserName">labuser</Data> <Data Name="TargetDomainName">CORP-NET-A...</Data>	4798
<EventData xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <Data Name="TargetUserName">WDAGUtilityAccount</Data> <Data Name="TargetDomainName">...</Data>	4798
<EventData xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <Data Name="TargetUserName">labuser</Data> <Data Name="TargetDomainName">CORP-NET-A...</Data>	4798
<EventData xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <Data Name="TargetUserName">Guest</Data> <Data Name="TargetDomainName">CORP-NET-AU...</Data>	4798
<EventData xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <Data Name="TargetUserName">DefaultAccount</Data> <Data Name="TargetDomainName">CORP...</Data>	4798
<EventData xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <Data Name="TargetUserName">labuser</Data> <Data Name="TargetDomainName">CORP-NET-A...</Data>	4798
<EventData xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <Data Name="TargetUserName">Administrators</Data> <Data Name="TargetDomainName">Builtin...</Data>	4799
<EventData xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <Data Name="TargetUserName">Remote Desktop Users</Data> <Data Name="TargetDomainName">...</Data>	4799
	4672

11. Creating the Threat Map

Create a threat map using Workbooks that references the watchlist you imported (network/location data). Build an interactive map showing attacking locations and relevant metrics, save the workbook, and revisit the underlying query anytime. For example, you might see large volumes—e.g., 22,000 events from a single IP range (And this was only within 4 hours!) —with location mismatches (Argentina vs. some connections from Ukraine), suggesting proxying or botnet activity.

The screenshot shows the Microsoft Defender Home interface with the 'Workbooks' section selected. The left sidebar remains the same as the previous screenshot. The main area shows 'My workbooks' with 0 workbooks, 'Templates' with 2 templates, and 'Updates' with 0 updates. It includes a 'Content hub' link. Below this, there's a section titled 'Microsoft Sentinel Workbooks' with a 'What is it?' description. It explains that workbooks enable instant visualization and analysis across connected data sources, providing full power of tools with tables and charts. It also links to 'Learn more about Workbooks' and 'Learn more about OOTB content and Content hub'.

New Workbook

No items.

+ Add ▾

[Done Editing](#) | [Advanced editor](#) OFF

New Workbook

Done Editing Advanced editor Refresh Auto refresh Off

Editing query - 0

Query Settings Visual Formatting Step Settings Advanced Editor

Show below is a JSON representation of the current doc. Any changes you make here will be reflected when you press Apply.

```
[{"$schema": "https://aka.ms/powerbi/datasourcequery", "version": 1, "datasets": [{"name": "SecurityEvent", "uri": "https://api.usgovcloud.us/microsoft/operationalinsights/v1/workspaces/SecurityEvent/_tables($t1)/SecurityEvent", "lastUpdated": "2023-07-10T14:45:00Z"}, {"name": "NetworkLog", "uri": "https://api.usgovcloud.us/microsoft/operationalinsights/v1/workspaces/NetworkLog/_tables($t2)/NetworkLog", "lastUpdated": "2023-07-10T14:45:00Z"}], "query": "let geoip = _detachdataset("geoip"); let windowsevents = SecurityEvent|windowset events | where EventID == 4825| order-by TimeGenerated desc| evaluate ip2location(EventIP_Rule, IpAddress, NetworkName) summarize FailureCount = count() byIpAddress, latitude, longitude, cityname, countryname| project FailureCount, AttackerIP + ipAddress, latitude, longitude; geoip| join-left windowsevents on ipAddress; geoip| select ipAddress, FailureCount, AttackerIP, latitude, longitude, cityname, countryname; geoip| summarize FailureCount = count() by cityname, countryname; geoip| project FailureCount, cityname, countryname; geoip| groupby {TimeGenerated} | summarize FailureCount = count() by TimeGenerated", "timeInterv": "PT1H", "duration": "PT24H"}, {"$schema": "https://aka.ms/powerbi/datasourcequery", "version": 1, "datasets": [{"name": "SecurityEvent", "uri": "https://api.usgovcloud.us/microsoft/operationalinsights/v1/workspaces/SecurityEvent/_tables($t1)/SecurityEvent", "lastUpdated": "2023-07-10T14:45:00Z"}, {"name": "NetworkLog", "uri": "https://api.usgovcloud.us/microsoft/operationalinsights/v1/workspaces/NetworkLog/_tables($t2)/NetworkLog", "lastUpdated": "2023-07-10T14:45:00Z"}], "query": "let geoip = _detachdataset("geoip"); let windowsevents = SecurityEvent|windowset events | where EventID == 4825| order-by TimeGenerated desc| evaluate ip2location(EventIP_Rule, IpAddress, NetworkName) summarize FailureCount = count() byIpAddress, latitude, longitude, cityname, countryname| project FailureCount, AttackerIP + ipAddress, latitude, longitude, cityname, countryname; geoip| join-left windowsevents on ipAddress; geoip| select ipAddress, FailureCount, AttackerIP, latitude, longitude, cityname, countryname; geoip| summarize FailureCount = count() by cityname, countryname; geoip| project FailureCount, cityname, countryname; geoip| groupby {TimeGenerated} | summarize FailureCount = count() by TimeGenerated", "timeInterv": "PT1H", "duration": "PT24H"}]
```

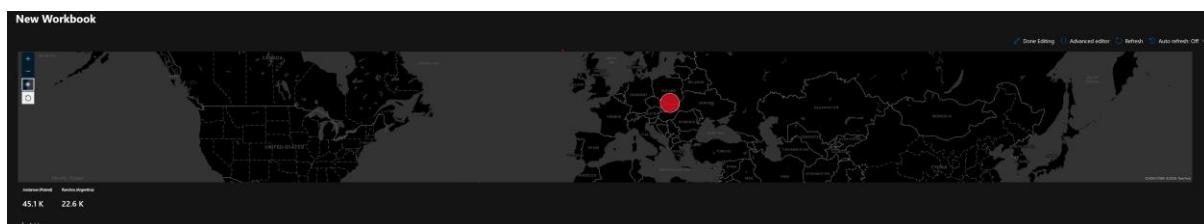
Apply

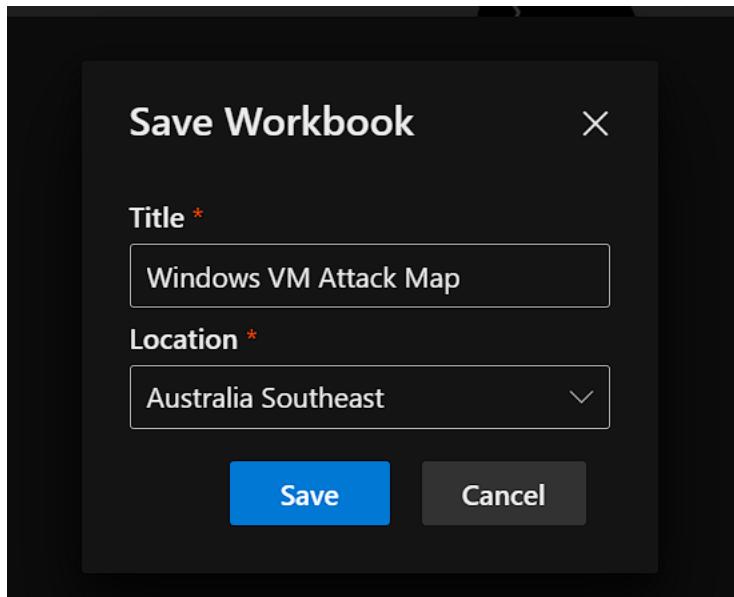
Add a title

Please run the Run Query button to use the data

Done Editing Cancel ...

+ Add





Results	Chart
1st GeoIPDB_FULL = getGeoList("geoip");	
SecurityEvent	
SecurityEventID == 4452	
where IpAddress == "192.241.96.63"	
evaluate Ipvc_localhost(GeoIPDB_Full, IpAddress, network)	
order by TimeGenerated desc	

Geolocation data from	IP2Location	Product: DB6, 2026-1-15
IP ADDRESS: 185.243.96.63	ISP: Demenin B.V.	
COUNTRY: Ukraine	ORGANIZATION: Not available	
REGION: Dnipropetrovska oblast	LATITUDE: 48.4500	
CITY: Dnipro	LONGITUDE: 34.9830	
Incorrect location?	Contact IP2Location	view map

Geolocation data from	ipinfo.io	Product: API, real-time
IP ADDRESS: 185.243.96.63	ISP: Not available	
COUNTRY: Ukraine	ORGANIZATION: AS48693 Rices Privately owned enterprise	
REGION: Kyiv City	LATITUDE: 50.4547	
CITY: Kyiv	LONGITUDE: 30.5238	
Incorrect location?	Contact ipinfo.io	view map

Geolocation data from	DB-IP	Product: API, real-time
IP ADDRESS: 185.243.96.63	ISP: Rices Privately owned enterprise	
COUNTRY: Ukraine	ORGANIZATION: Rices Privately owned enterprise	
REGION: Dnipropetrovsk	LATITUDE: 48.4647	
CITY: Dnipro	LONGITUDE: 35.0462	
Incorrect location?	Contact DB-IP	view map

Geolocation data from	IPregistry.co	Product: API, real-time
IP ADDRESS: 185.243.96.63	ISP: Rices Privately Owned Enterprise	
COUNTRY: Ukraine	ORGANIZATION: Rices Privately Owned Enterprise (ntup.net)	
REGION: Kyiv	LATITUDE: 50.45478	
CITY: Kyiv	LONGITUDE: 30.52376	
Incorrect location?	Contact IPregistry.co	view map

Query: "let GeolPDB_FULL = _GetWatchlist("geoip");

SecurityEvent

```
| where EventID == 4625  
| where ipAddress == "185.243.96.63"  
| evaluate ipv4_lookup(GeoIPDB_FULL, ipAddress, network)  
| order by TimeGenerated desc"
```

Map: {"

```
    "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"
}
```

```

After we are done, we remove the resource group and virtual machine.

| Operation name                                    | Status  | Time           | Time since   | Subscription         | Event initiated by   |
|---------------------------------------------------|---------|----------------|--------------|----------------------|----------------------|
| Create or update Virtual Network                  | Success | 4 minutes ago  | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| Delete Network Interface                          | Success | 4 minutes ago  | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| Deallocate Virtual Machine                        | Success | 16 minutes ago | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| Create or update workload                         | Success | 18 minutes ago | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| New recommendation is available                   | Success | 26 minutes ago | Now (Feb 02) | Azure subscription 1 | Microsoft Advisor    |
| Create Workloads                                  | Success | 3 hours ago    | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| Create Workload                                   | Success | 3 hours ago    | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| Create or update Application                      | Success | 3 hours ago    | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| Create or update Virtual Machine Extension        | Success | 3 hours ago    | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| Create or update Data collection rule             | Success | 3 hours ago    | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| Create new CMS solution                           | Success | 3 hours ago    | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| Create or update Data collection role association | Success | 3 hours ago    | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| Get deployment operation status                   | Success | 3 hours ago    | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| Create Deployment                                 | Success | 3 hours ago    | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| Update Deployment                                 | Success | 3 hours ago    | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| Get deployment operation status                   | Success | 3 hours ago    | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| Get deployment operation status                   | Success | 3 hours ago    | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| Get deployment operation status                   | Success | 3 hours ago    | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| Update Orchestration States                       | Success | 3 hours ago    | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| Region Microsoft Insights                         | Success | 3 hours ago    | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| Region Subscription                               | Success | 3 hours ago    | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| Create Deployment                                 | Success | 3 hours ago    | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| Update Deployment                                 | Success | 3 hours ago    | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| Region Subscription                               | Success | 3 hours ago    | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| Vehicle Deployment                                | Success | 3 hours ago    | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| Region Subscription                               | Success | 3 hours ago    | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| Create or Update Security Rule                    | Success | 3 hours ago    | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| Delete Security Rule                              | Success | 3 hours ago    | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |
| Update/Replace Policy actions                     | Success | 7 hours ago    | Now (Feb 02) | Azure subscription 1 | MicrosoftCompute/... |