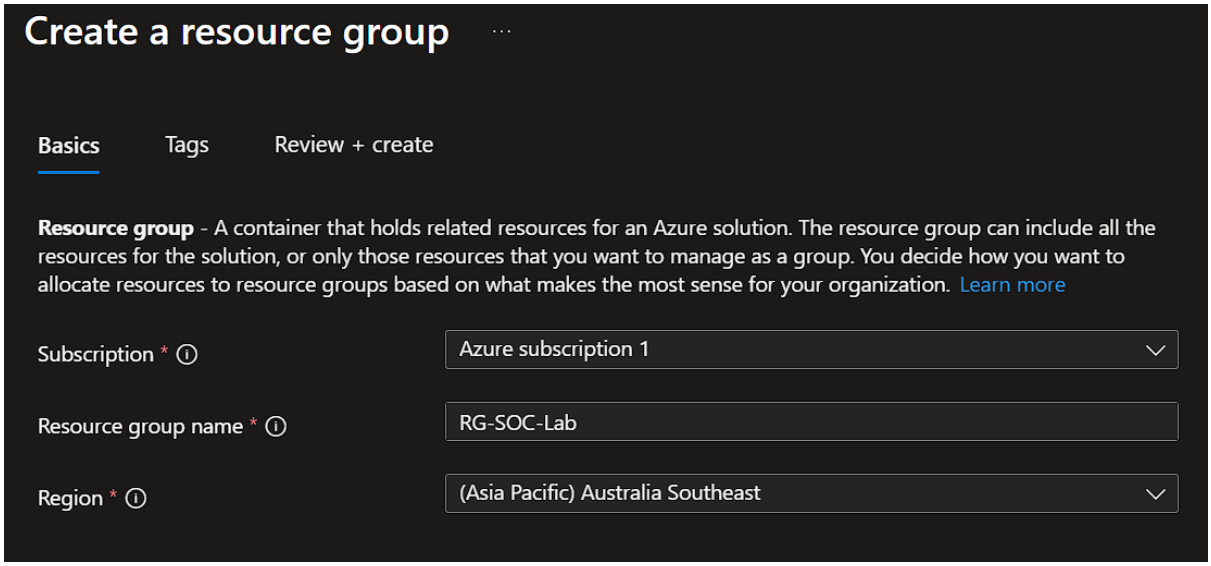
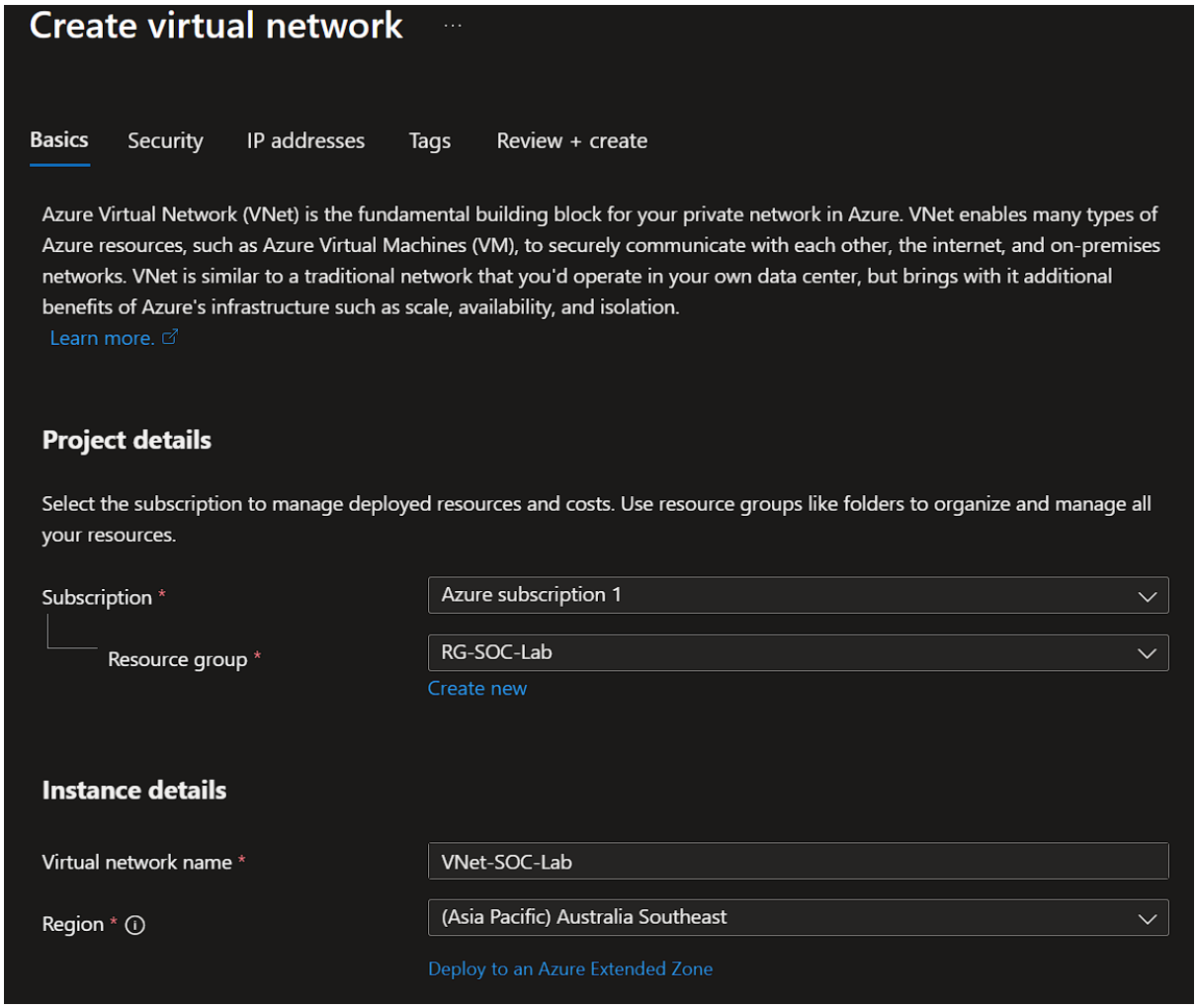
Creating a Honeypot with Azure and Microsoft Sentinel

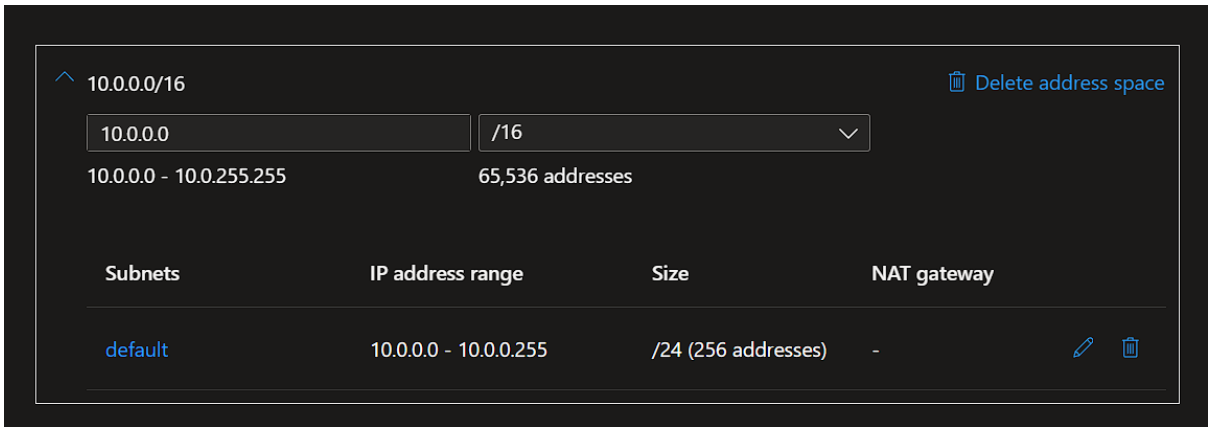
1. Create the Resource Group



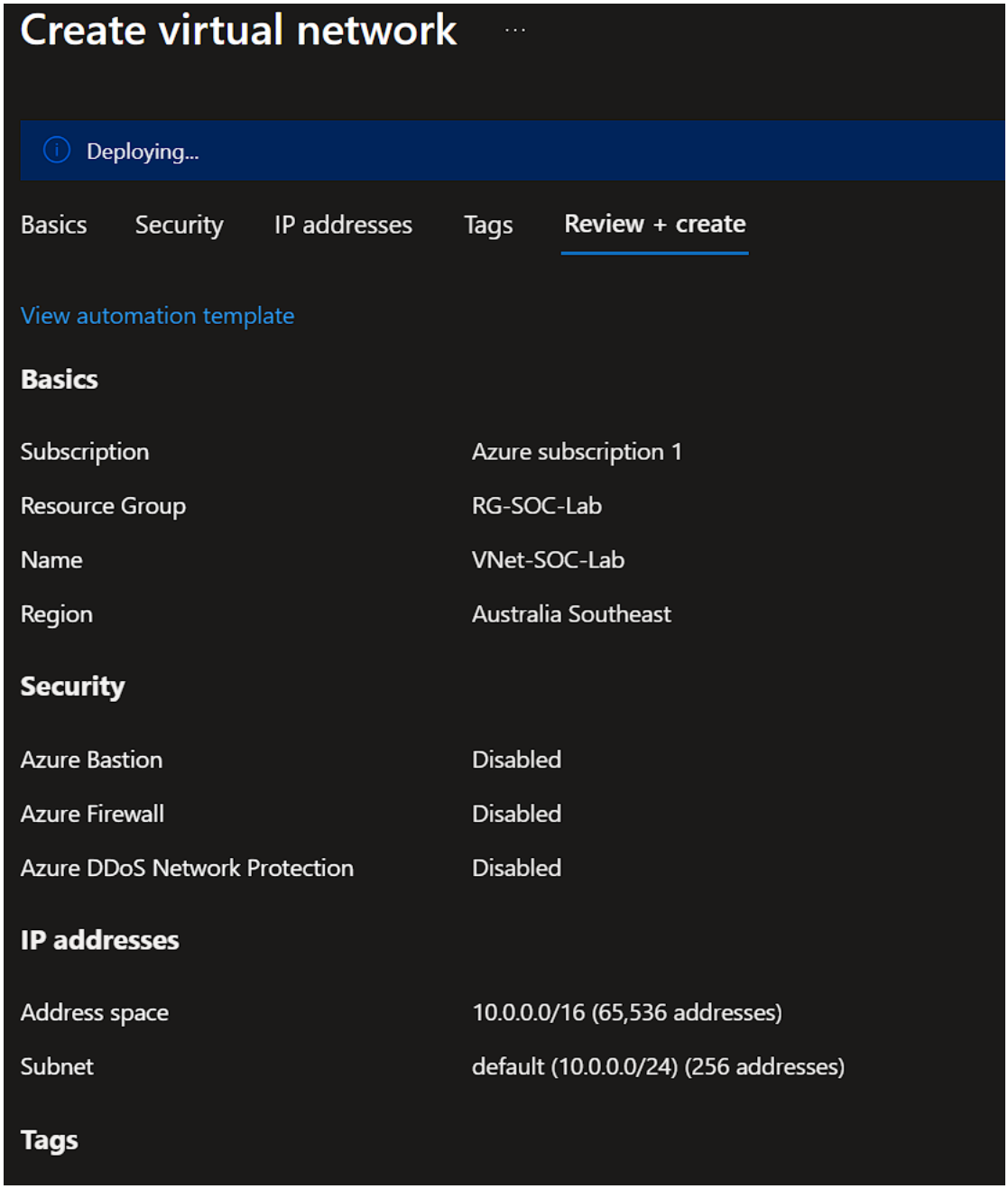
You need an active Azure subscription. After subscribing, create a resource group in your preferred region and give it a distinctive name for easy identification — for example: **RG-SOC-Lab**.

2. Create the Virtual Network





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**.



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 lo

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

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

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 * : ••••••••••••

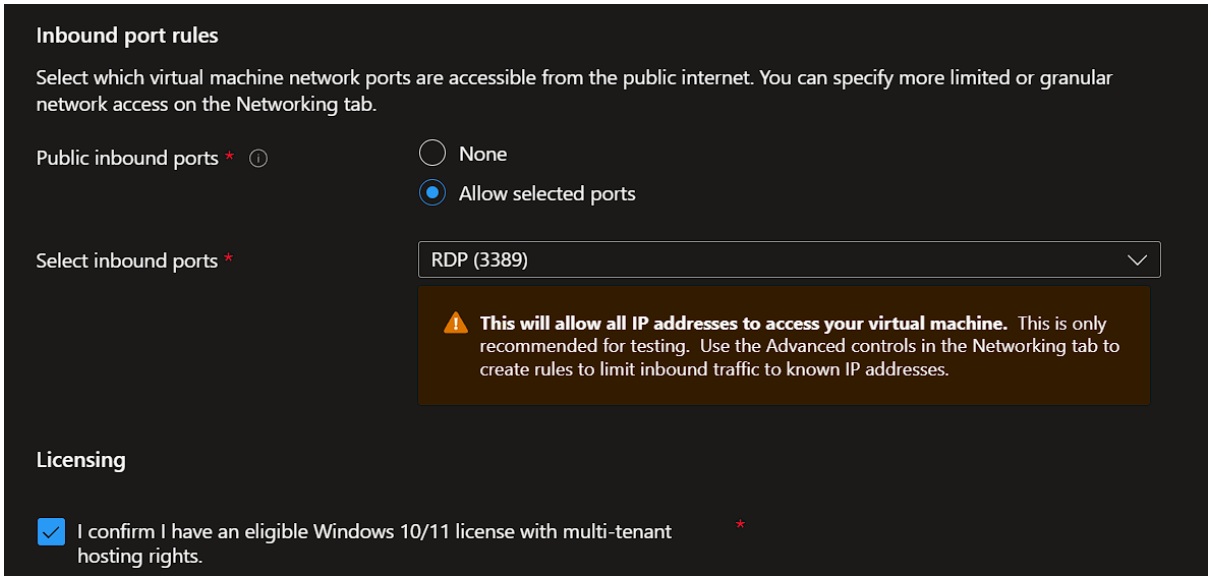
Confirm password * : ••••••••••••

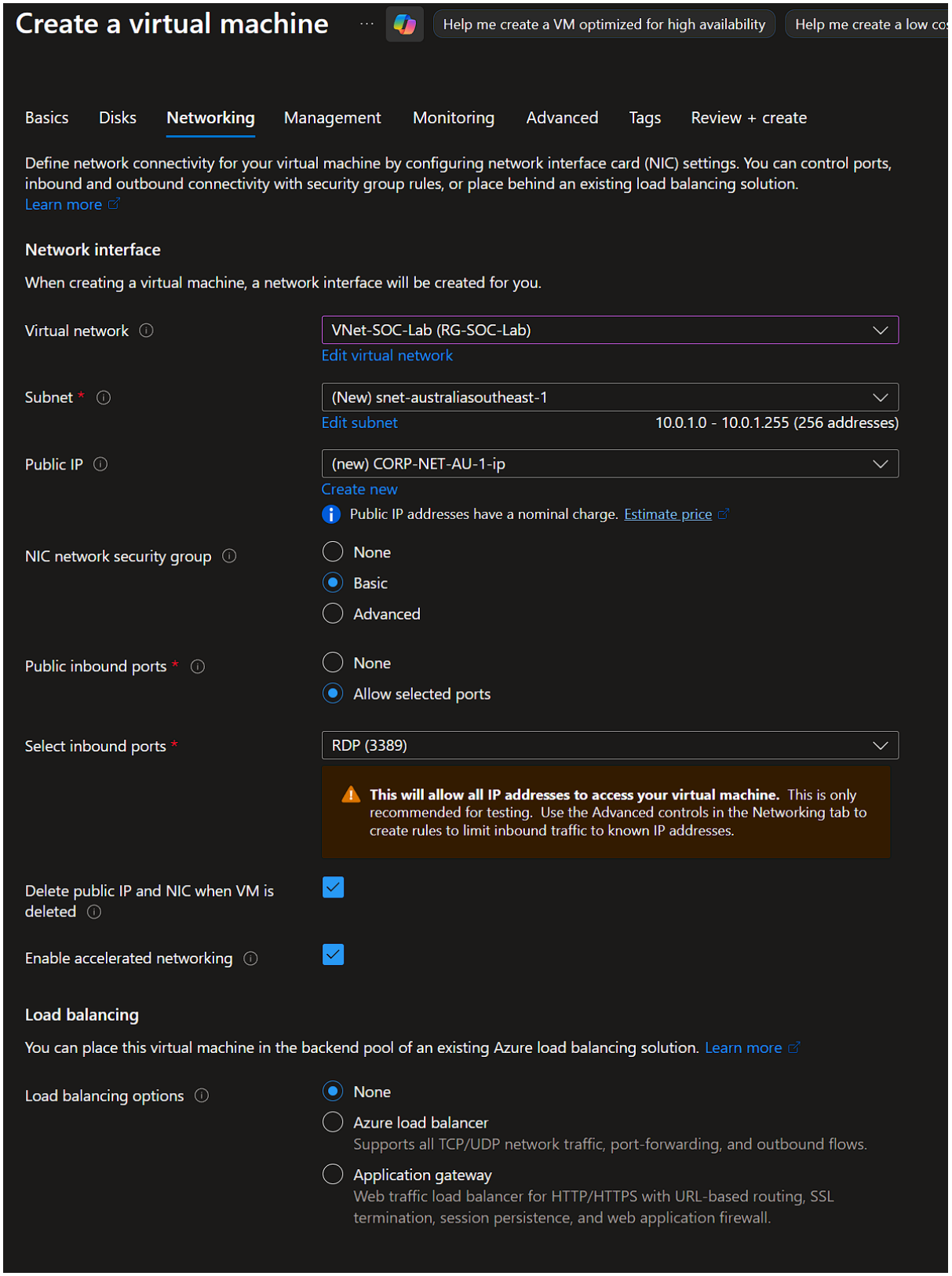
Inbound port rules

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 co
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 lov

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

Subscription credits apply

0.1250 USD/hr

Pricing for other VM sizes

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.

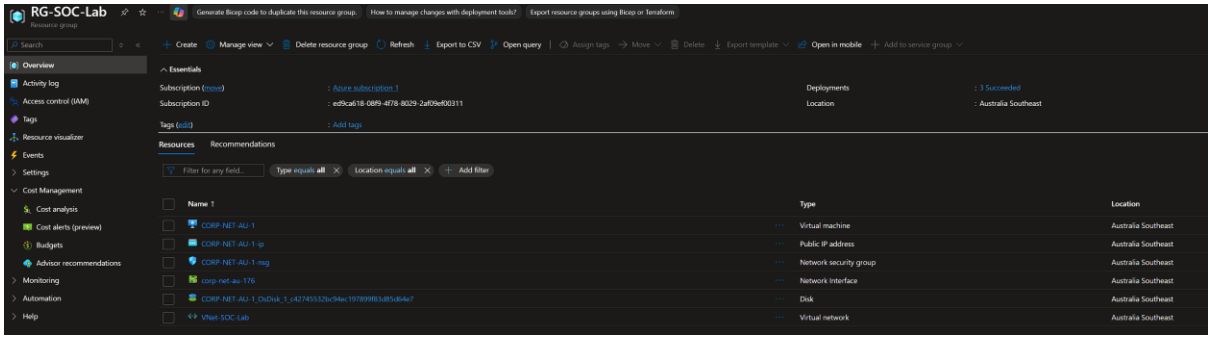
You have set RDP port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.

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

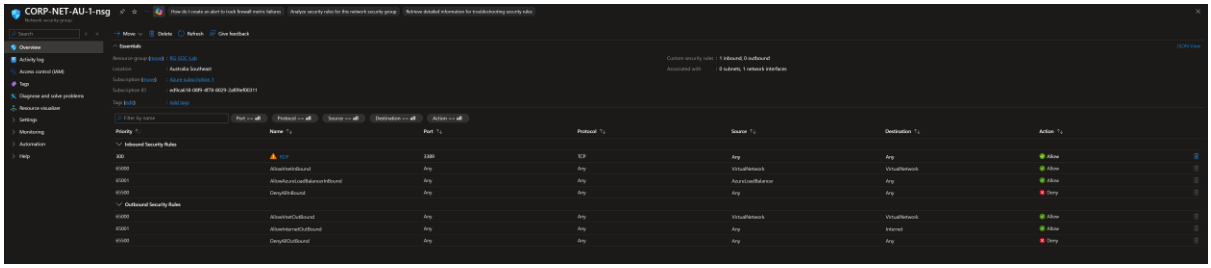
Disks

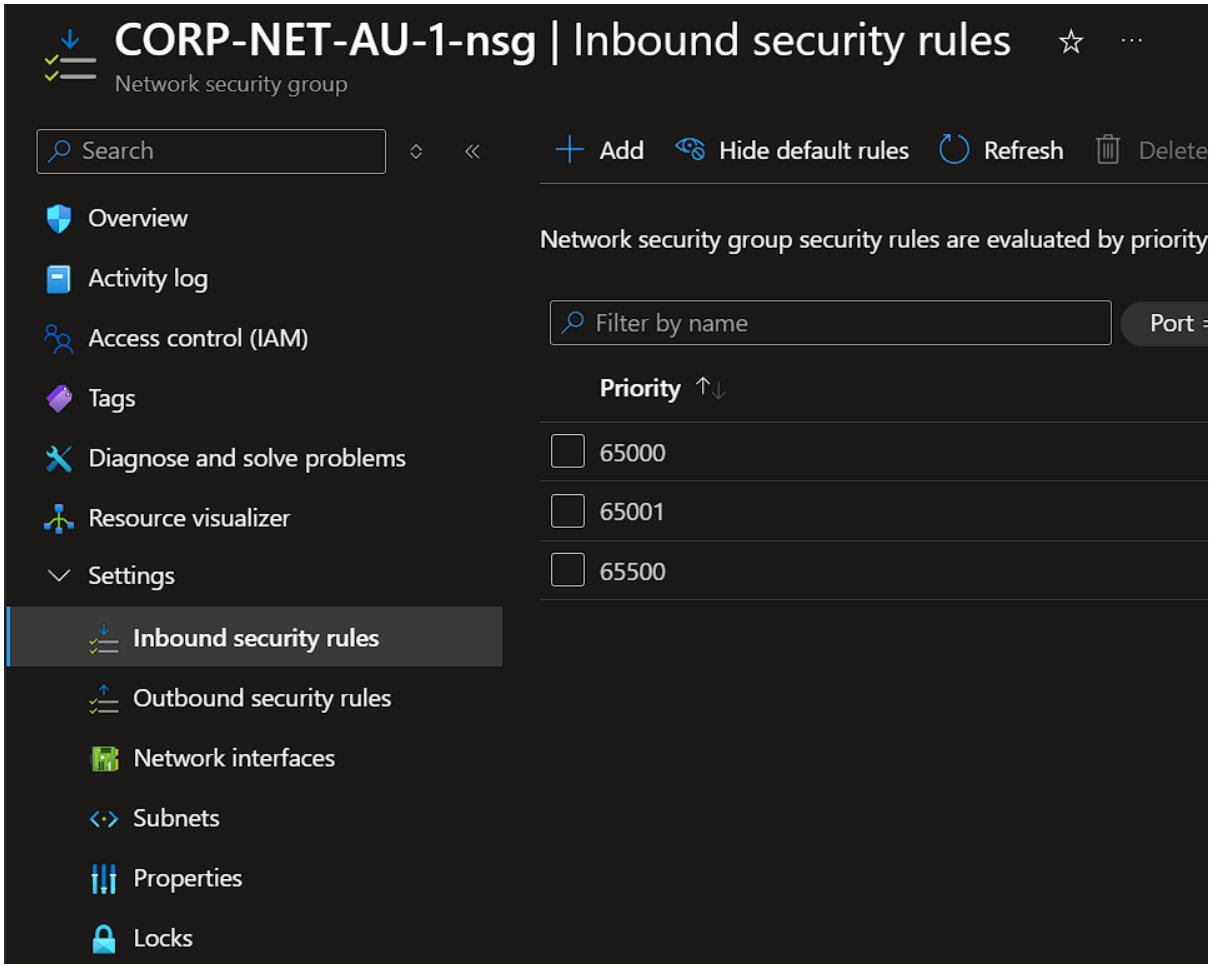
OS disk size	Image default
OS disk type	Premium SSD LRS
Use managed disks	Yes

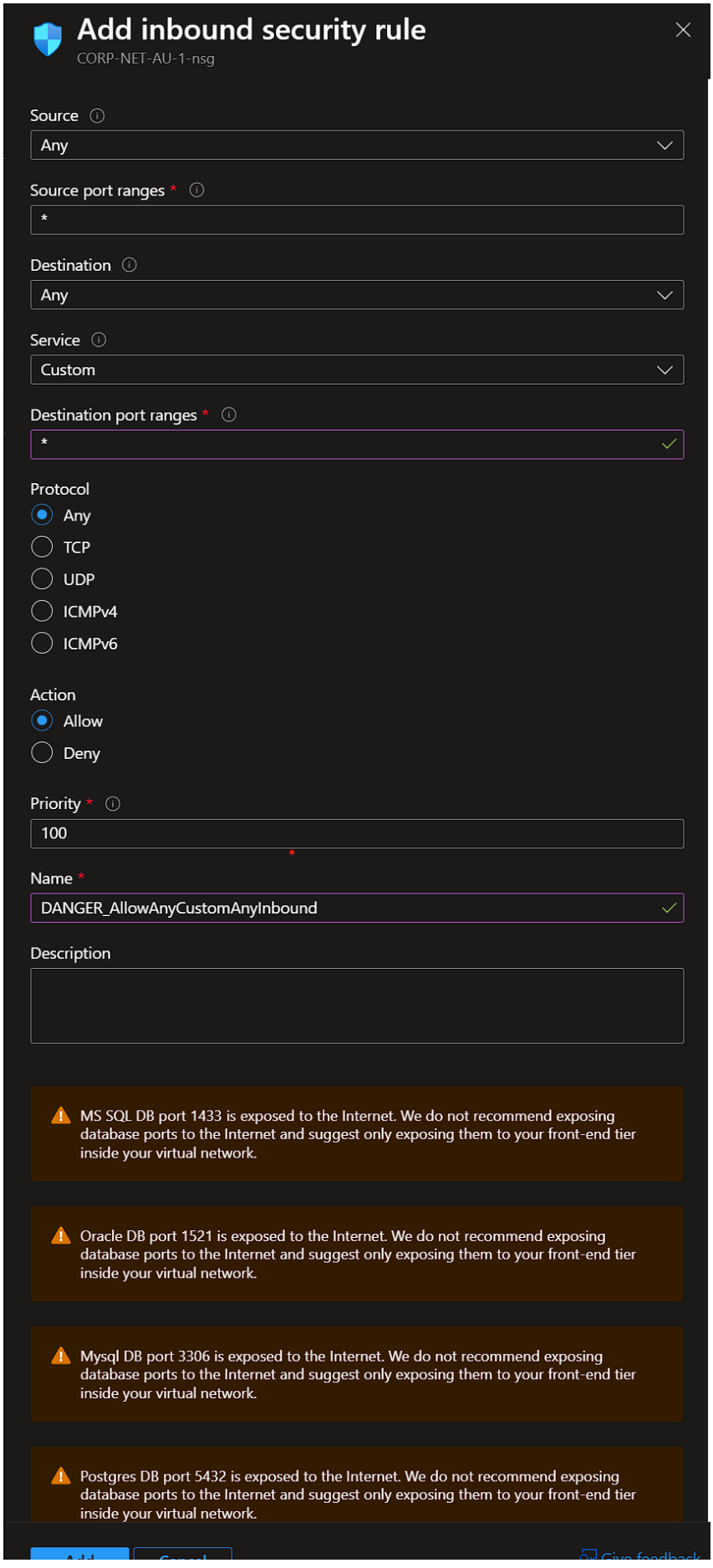


4. Expose VM to the Internet

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**.

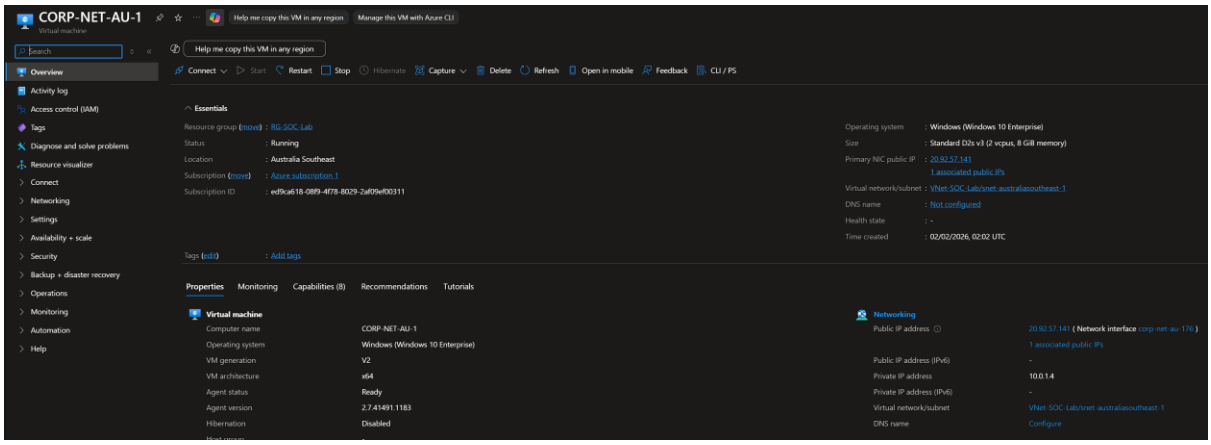


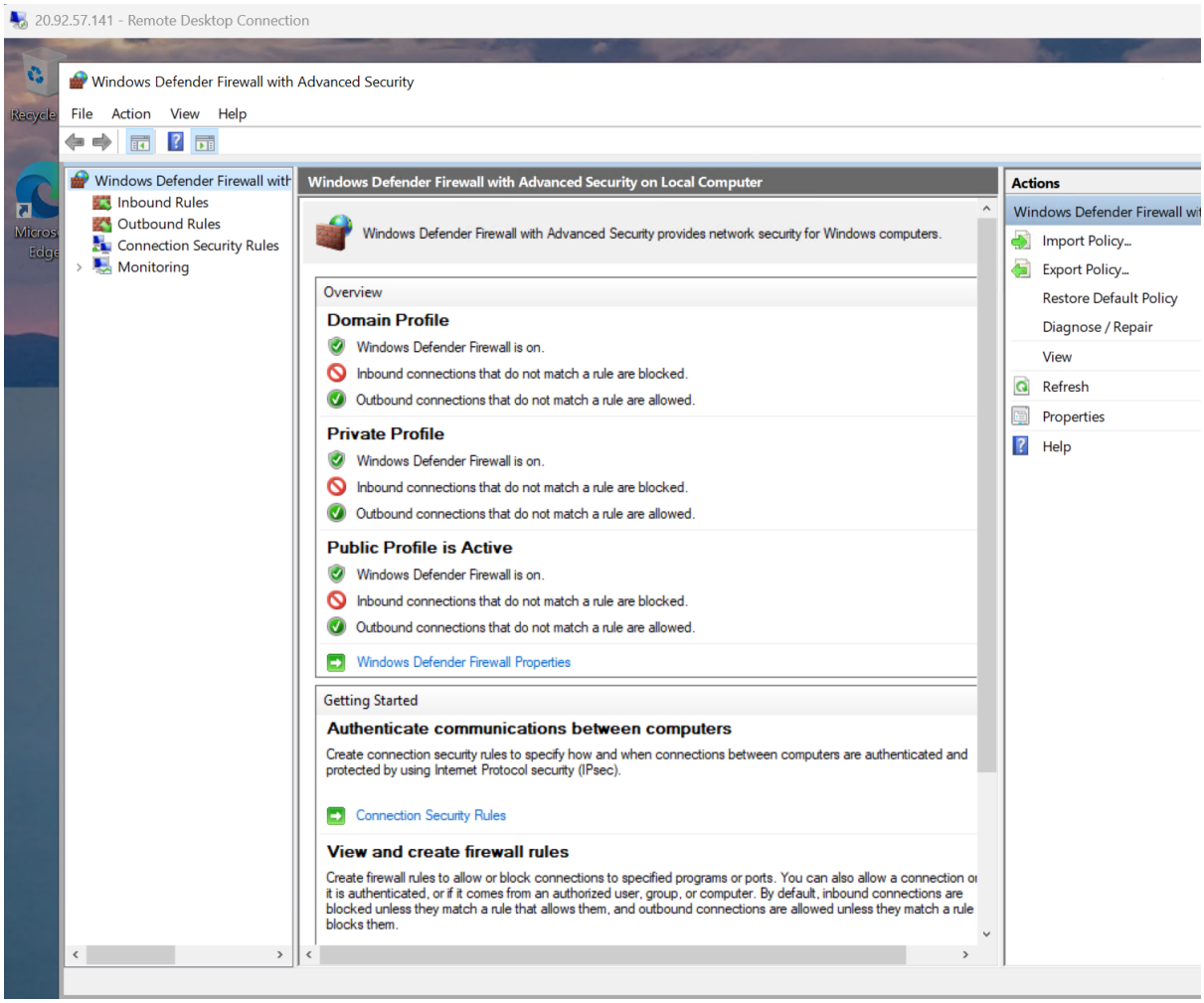

CORP-NET-AU-1-nsg | Inbound security rules
Network security group
Search
Add
Hide default rules
Refresh
Delete
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Network security group security rules are evaluated by priority
Filter by name
Port
Priority
65000
65001
65500

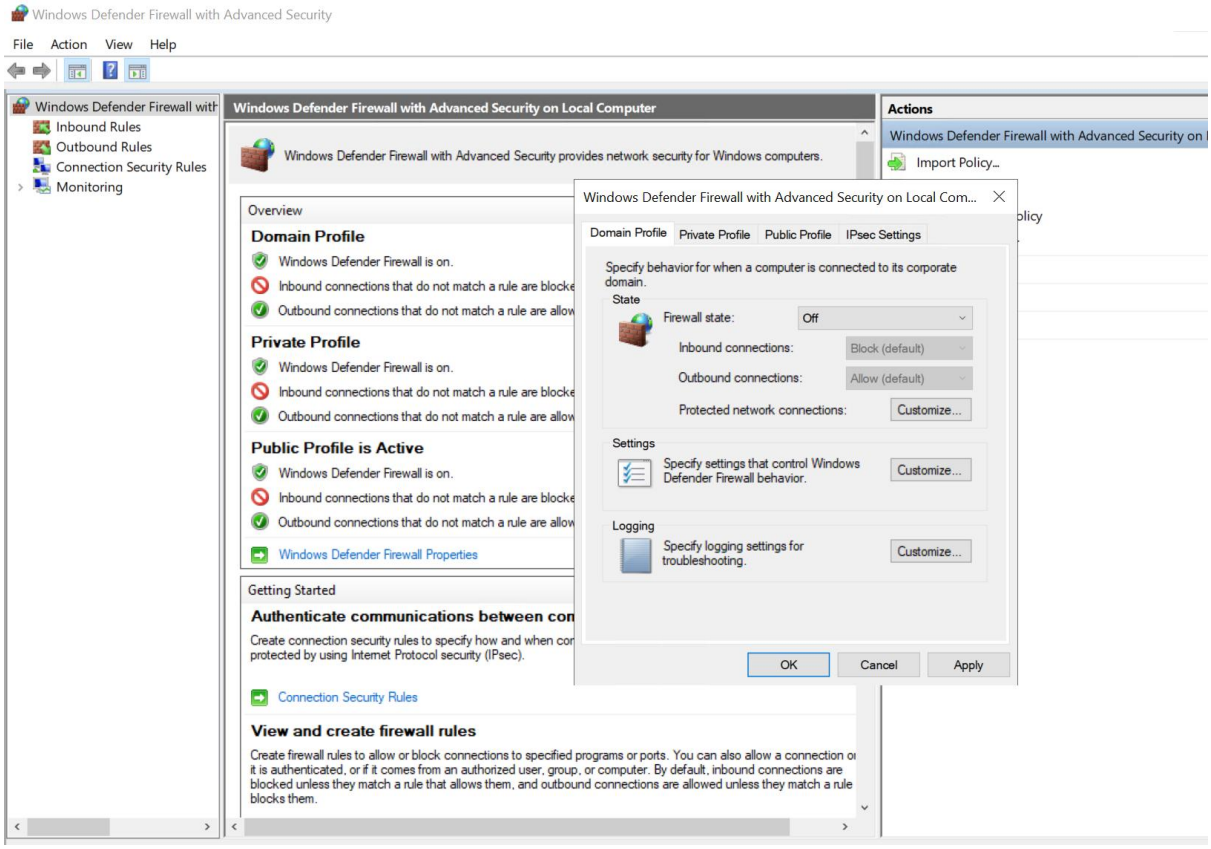

Add inbound security rule
CORP-NET-AU-1-nsg
Source
Any
Source port ranges *
*
Destination
Any
Service
Custom
Destination port ranges *
*
Protocol
Any
TCP
UDP
ICMPv4
ICMPv6
Action
Allow
Deny
Priority *
100
Name *
DANGER_AllowAnyCustomAnyInbound
Description
MS SQL DB port 1433 is exposed to the Internet. 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.

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.

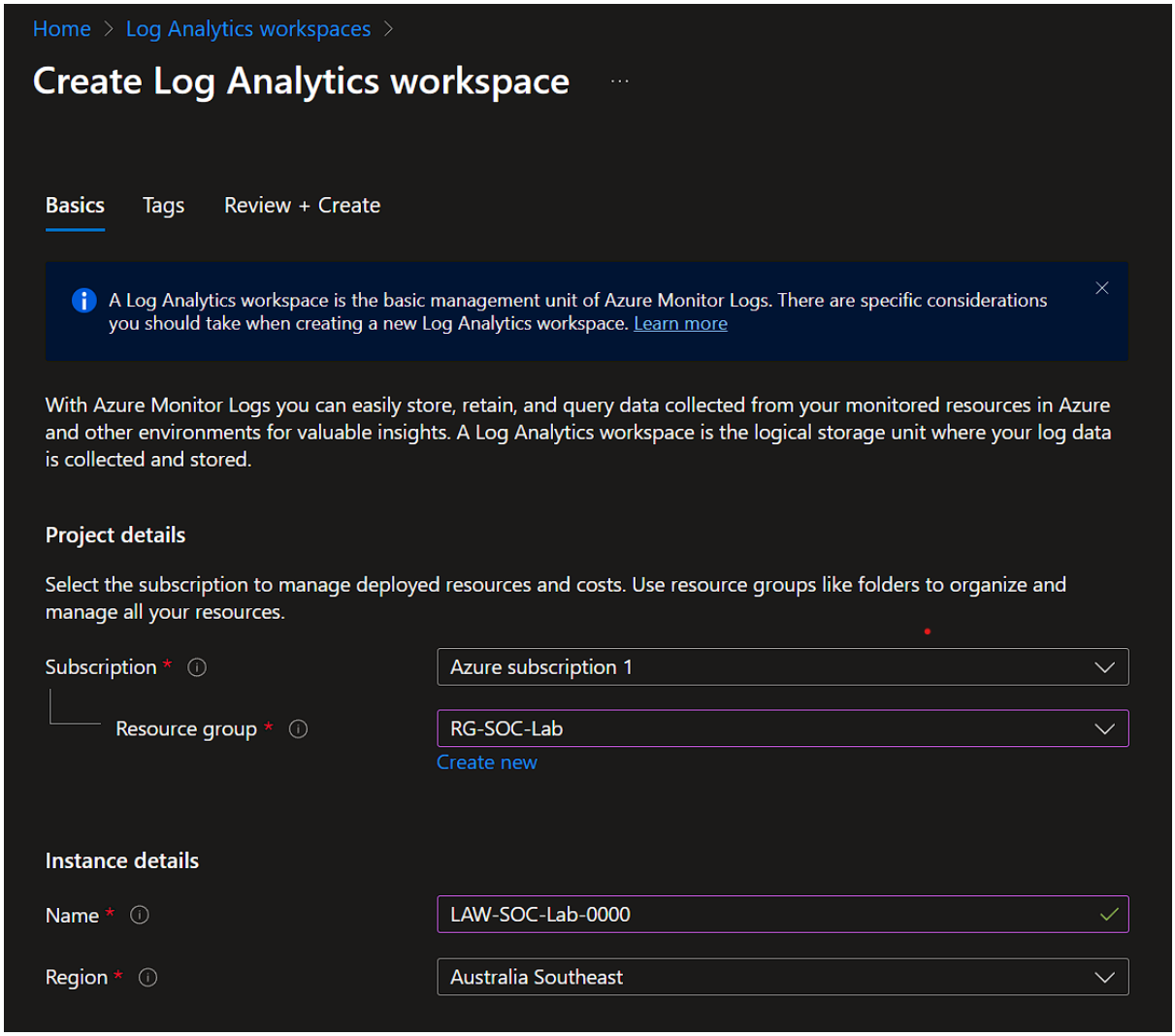






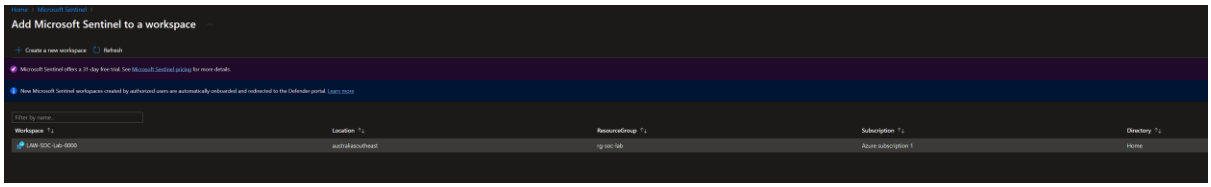
6. Creating the Log Analytics Workspace

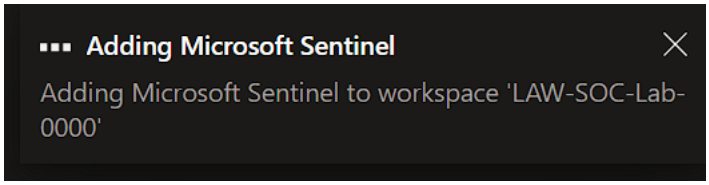
Create a Log Analytics workspace and connect it to the VM so it forwards events. Name the workspace **LAW-SOC-Lab-0000** for easy identification.



7. Linking Microsoft Sentinel

Proceed to link Microsoft Sentinel to the Log Analytics Workspace.

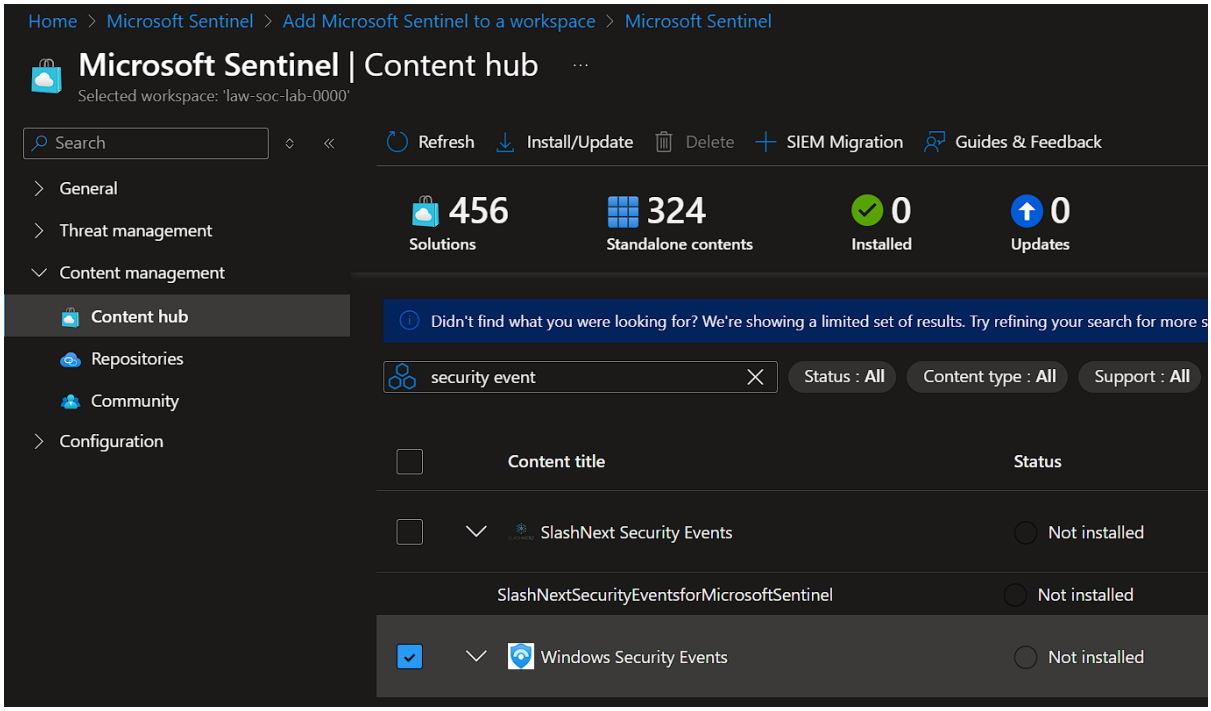




8. Connect VM to Log Analytics Workspace

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.



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

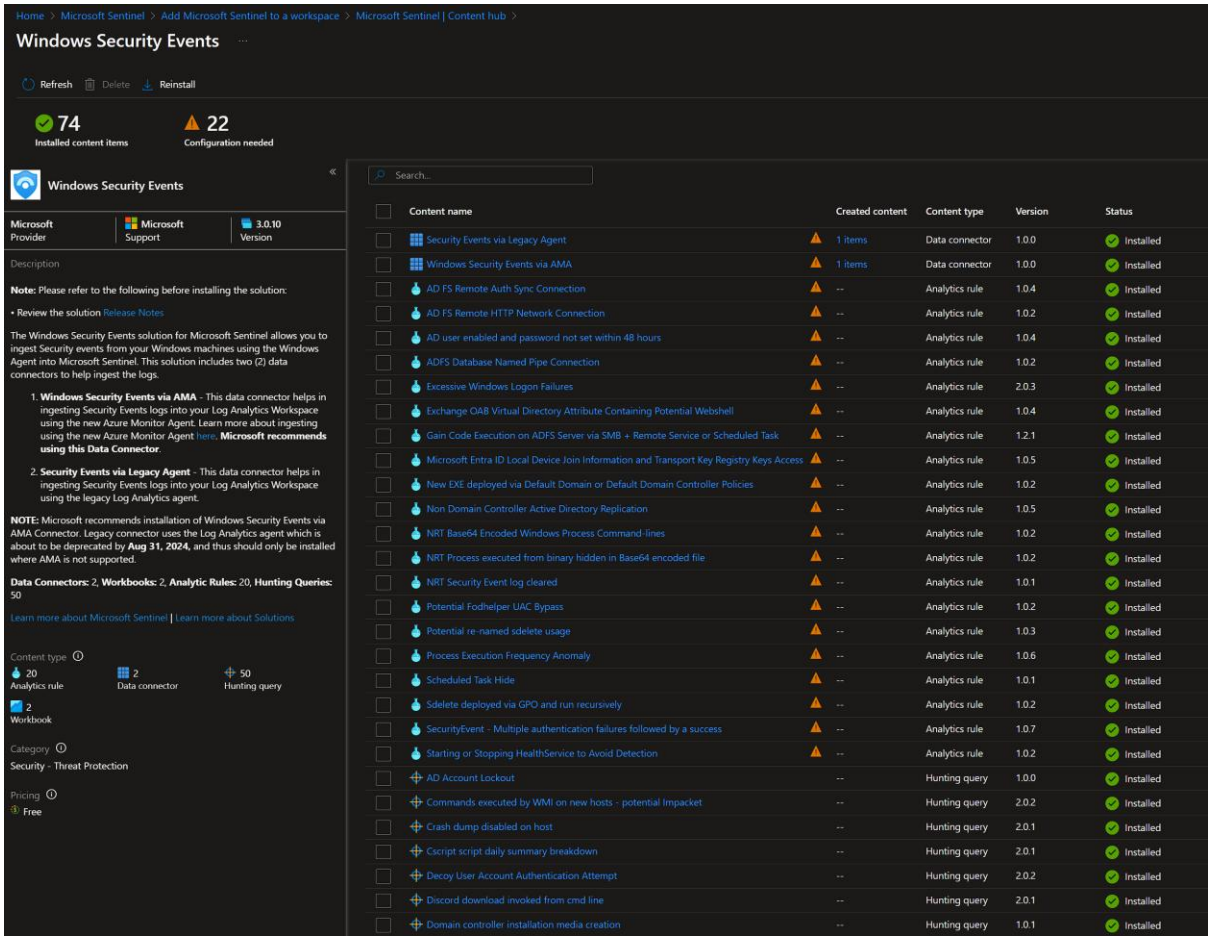
2
Workbook

Category

Security - Threat Protection

Pricing

Free


Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel | Content hub >
Windows Security Events
Refresh
Delete
Reinstall
74
Installed content items
22
Configuration needed
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
Search...
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 OAB 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
Cscript 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	Microsoft	--
Status	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

Windows Security Events

Version

1.0.0

Author

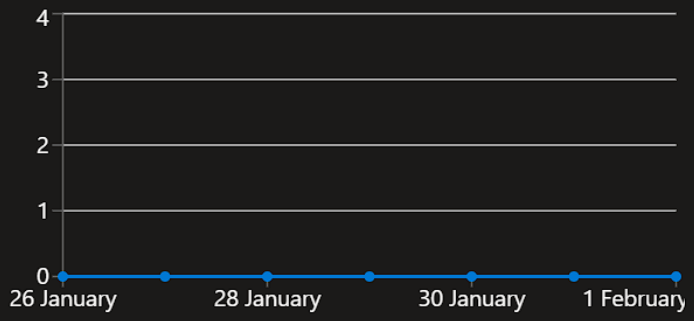
Microsoft

Supported by

Microsoft Corporation | Email

Data received

Go to query



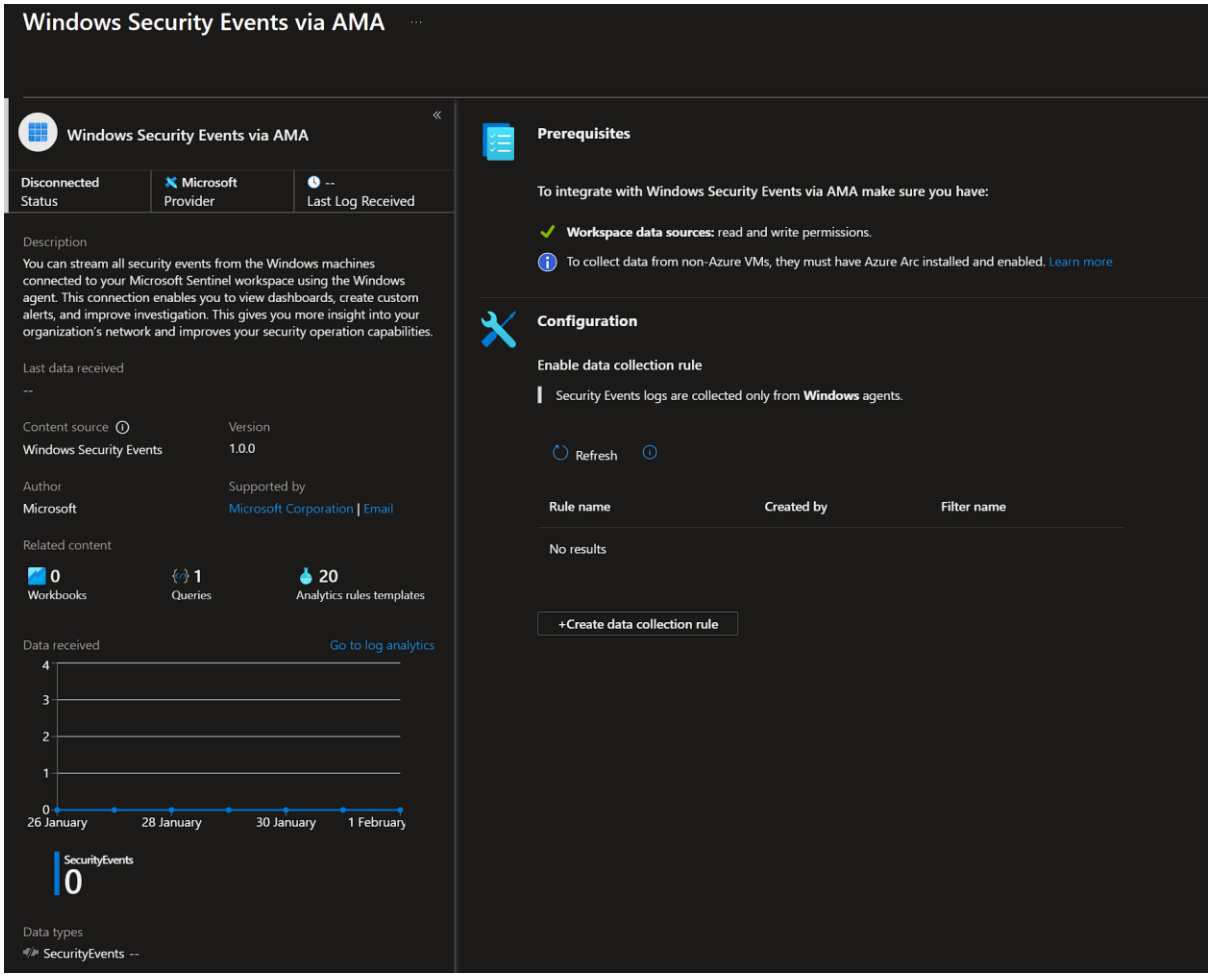
SecurityEvents

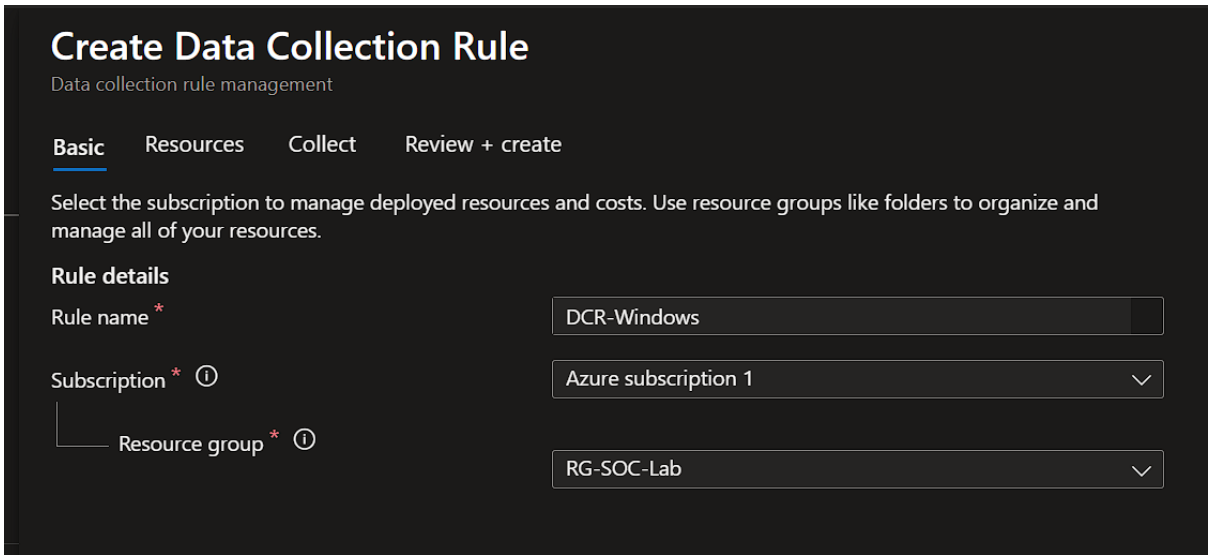
0

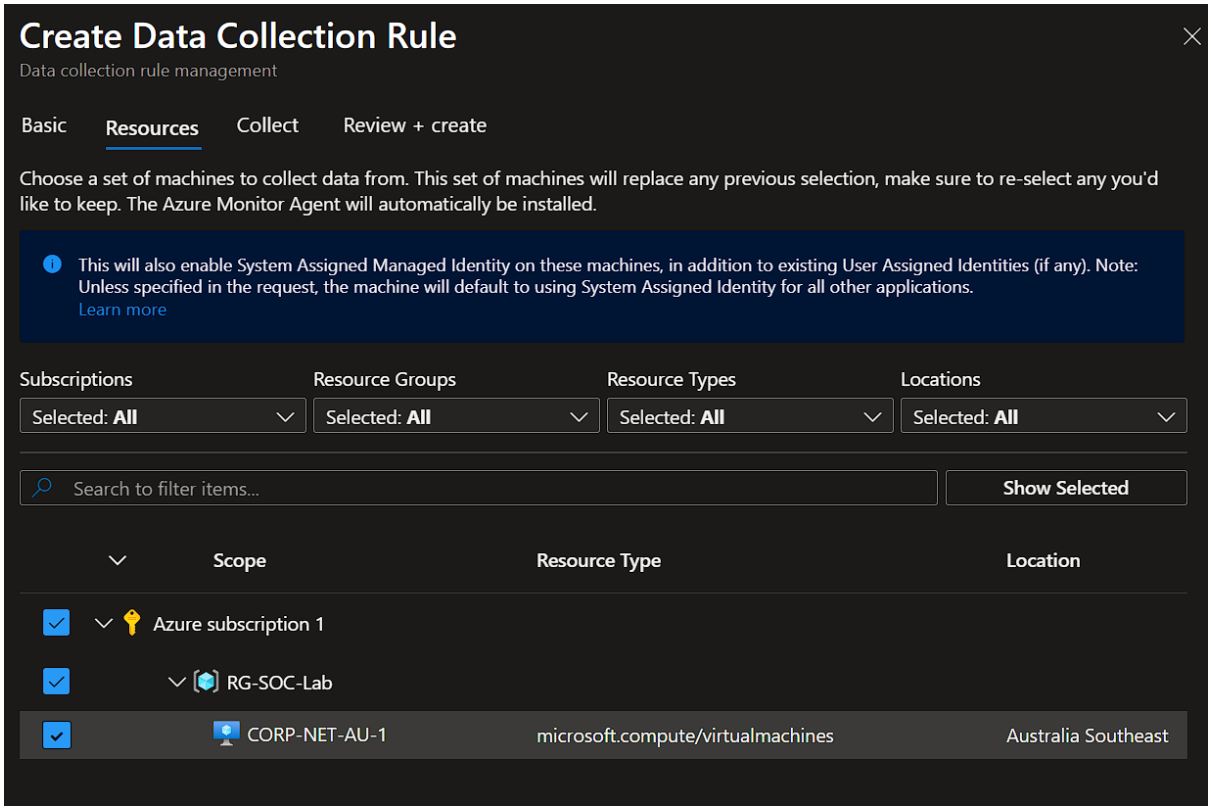
Data types

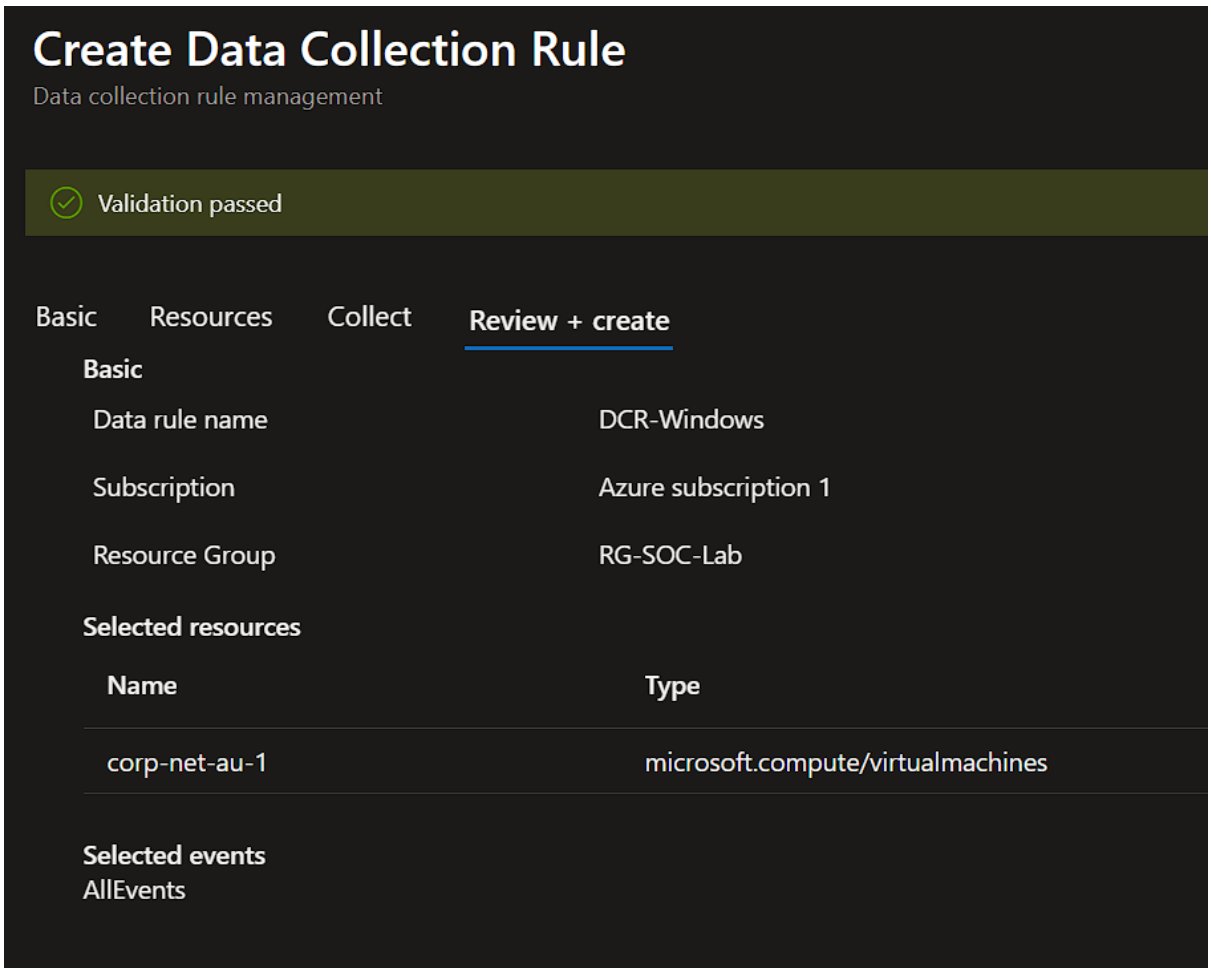
SecurityEvents --

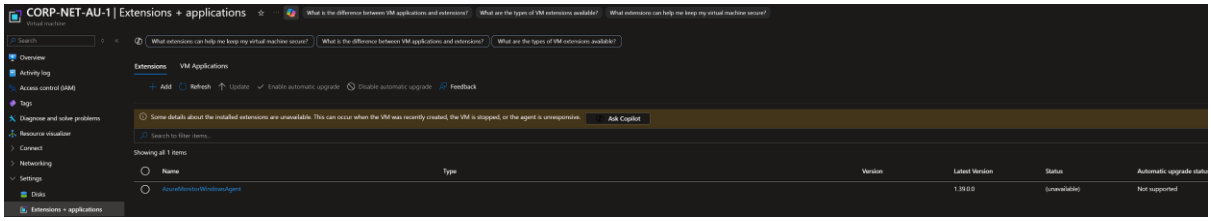
Open connector page


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
Windows Security Events
Version
1.0.0
Author
Microsoft
Supported by
Microsoft Corporation | Email
Related content
0
Workbooks
1
Queries
20
Analytics rules templates
Data received
Go to log analytics
4
3
2
1
0
26 January
28 January
30 January
1 February
SecurityEvents
0
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
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

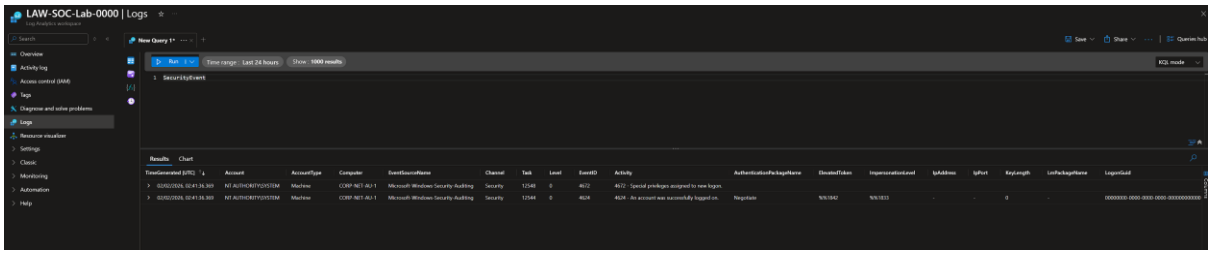

Create Data Collection Rule
Data collection rule management
Basic
Resources
Collect
Review + create
Choose a set of machines to collect data from. This set of machines will replace any previous selection, make sure to re-select any you'd like to keep. The Azure Monitor Agent will automatically be installed.
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
Selected: All
Resource Groups
Selected: All
Resource Types
Selected: All
Locations
Selected: All
Search to filter items...
Show Selected
Scope
Resource Type
Location
Azure subscription 1
RG-SOC-Lab
CORP-NET-AU-1
microsoft.compute/virtualmachines
Australia Southeast

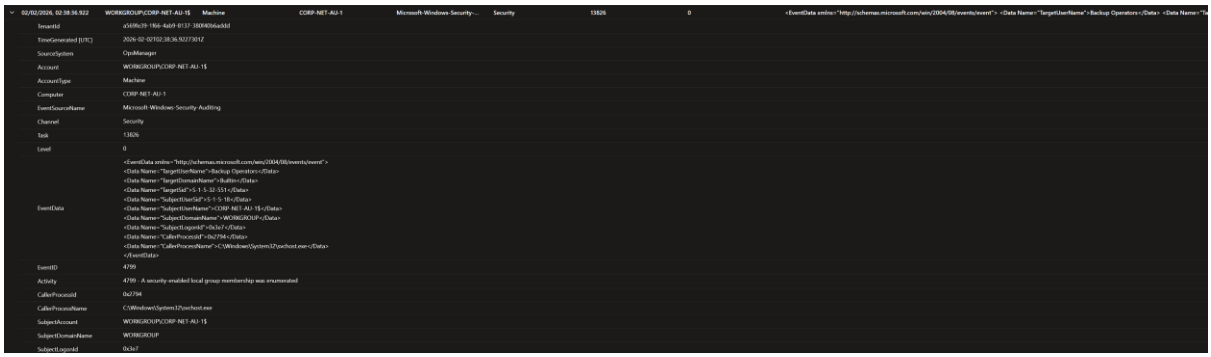

Create Data Collection Rule
Data collection rule management
Validation passed
Basic
Resources
Collect
Review + create
Basic
Data rule name
DCR-Windows
Subscription
Azure subscription 1
Resource Group
RG-SOC-Lab
Selected resources
Name
Type
corp-net-au-1
microsoft.compute/virtualmachines
Selected events
AllEvents



9. Querying with KQL

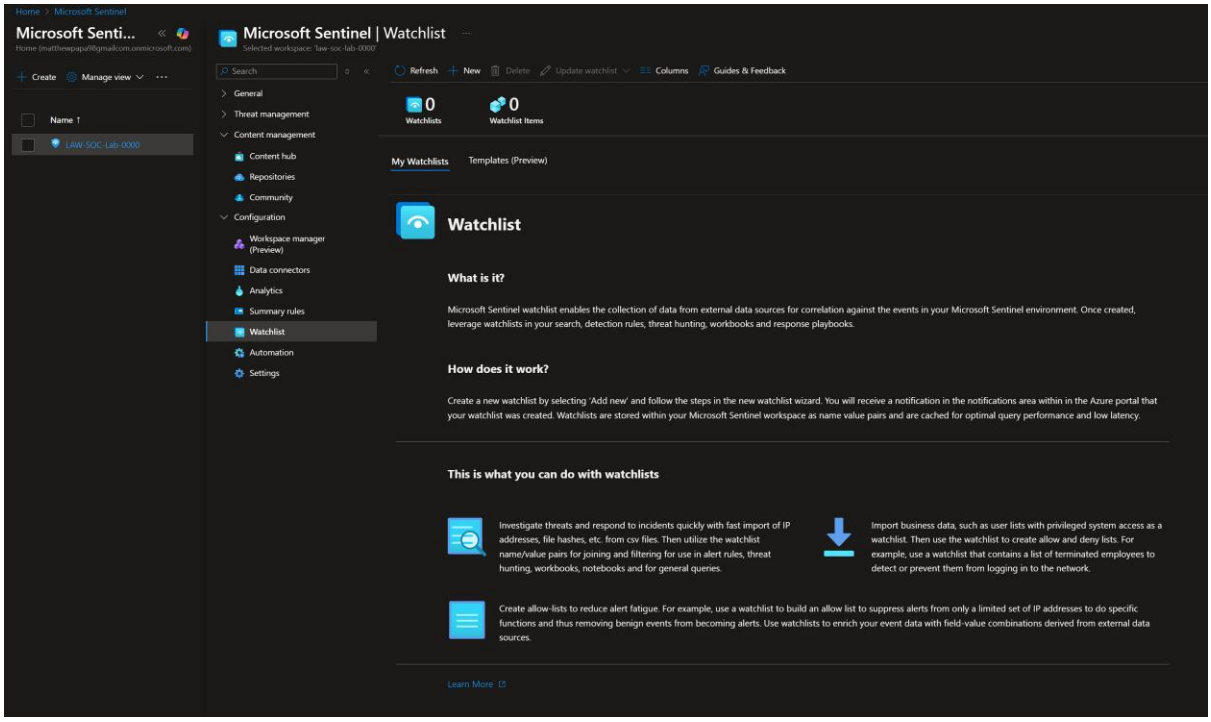
Start with basic KQL queries. Initial results show routine activity with no clear signs of compromise. However, after about five minutes—while creating the watchlist—suspicious activity began appearing, indicating probing attempts.



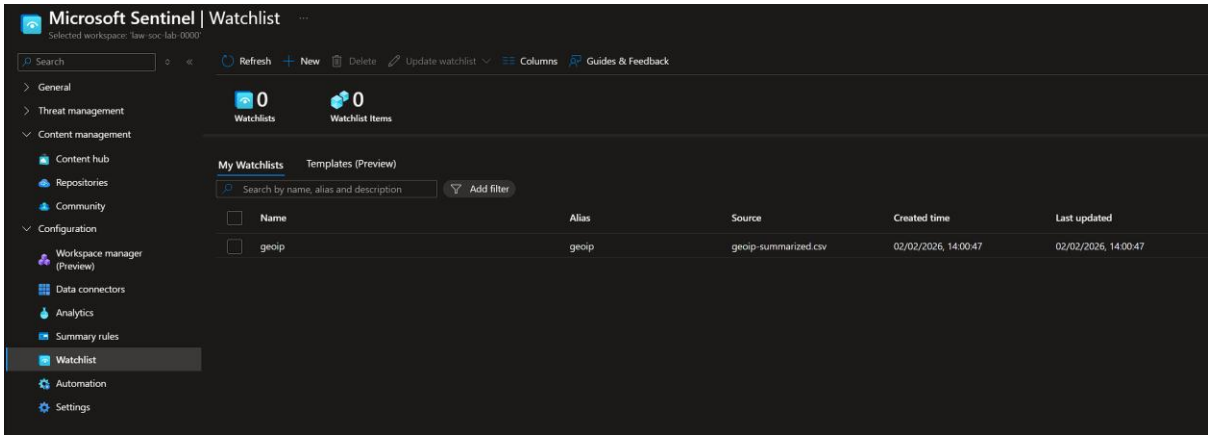


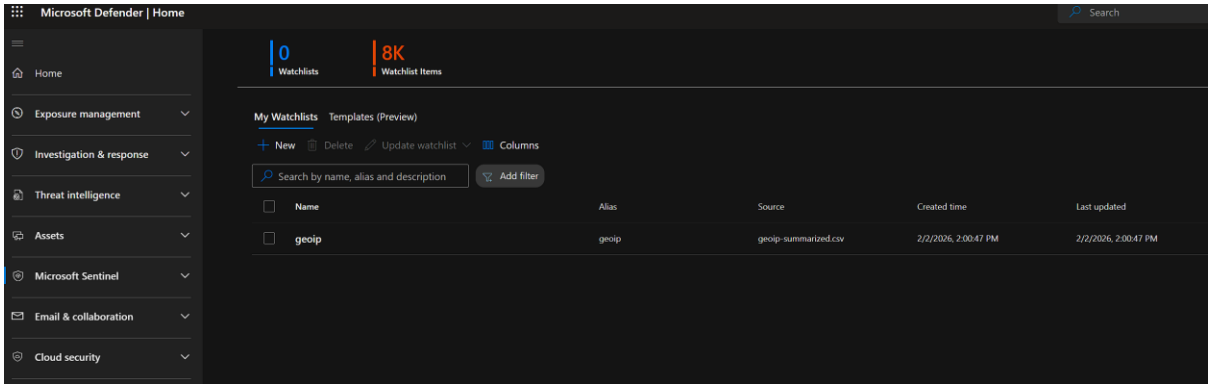
10. Creating the Watchlist

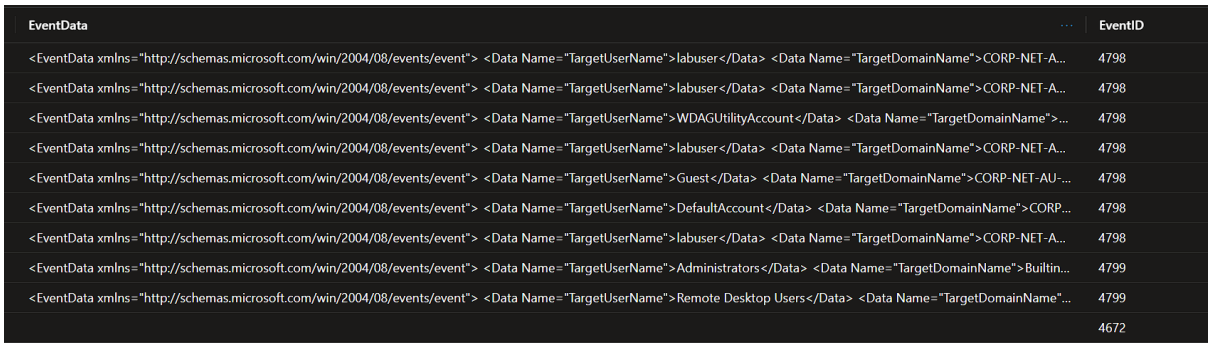
Create a watchlist in Microsoft Sentinel and upload a database file of locations and IPs (for example, MaxMind's GeoIP database). In production, this data would typically come from your provider's backend.


Microsoft Sentinel | Watchlist
Selected workspace: law-soc-lab-0000
Refresh
New
Delete
Update watchlist
Columns
Guides & Feedback
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


Microsoft Sentinel | Watchlist
Selected workspace: law-soc-lab-0000
Refresh
New
Delete
Update watchlist
Columns
Guides & Feedback
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

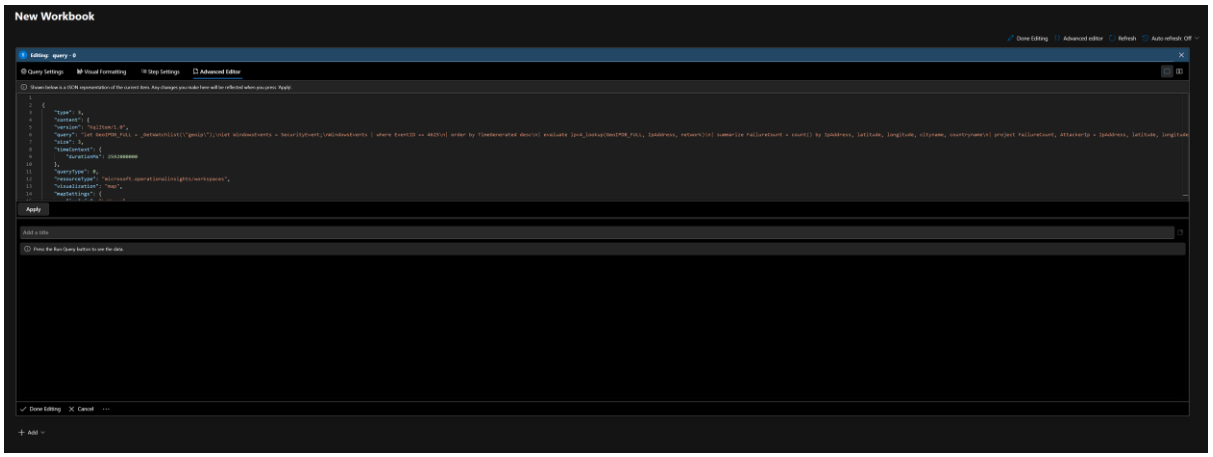


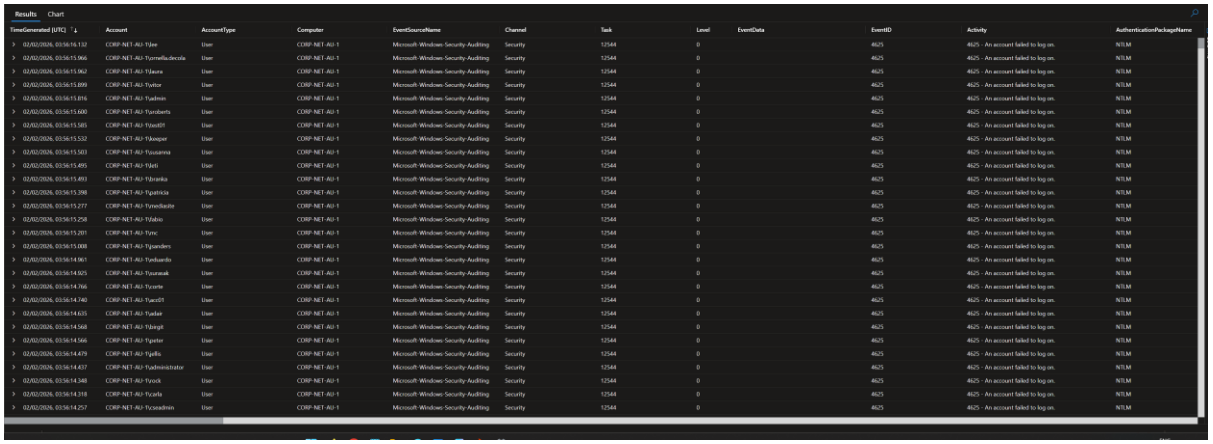


11. Creating the Threat Map

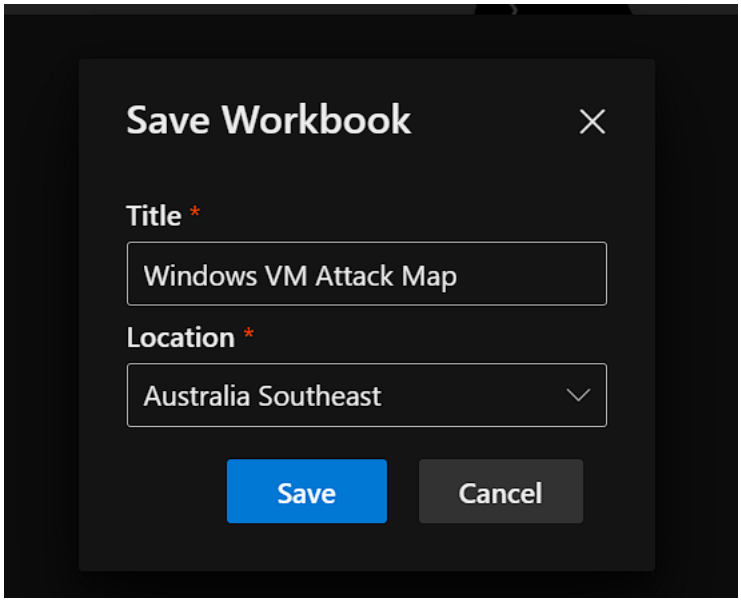
Create a threat map using Workbooks that references the watchlist you imported (network/location data). Build an interactive map showing attacking locations and relevant metrics, save the workbook, and revisit the underlying query anytime. For example, you might see large volumes—e.g., 22,000 events 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.

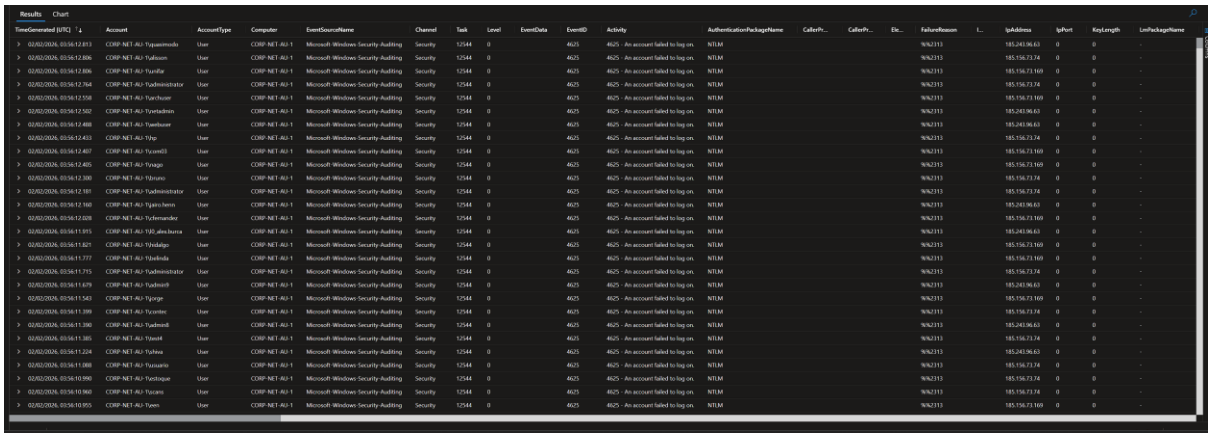

New Workbook
Done Editing
Advanced editor
Refresh
Auto refresh: Off
No items.
Add

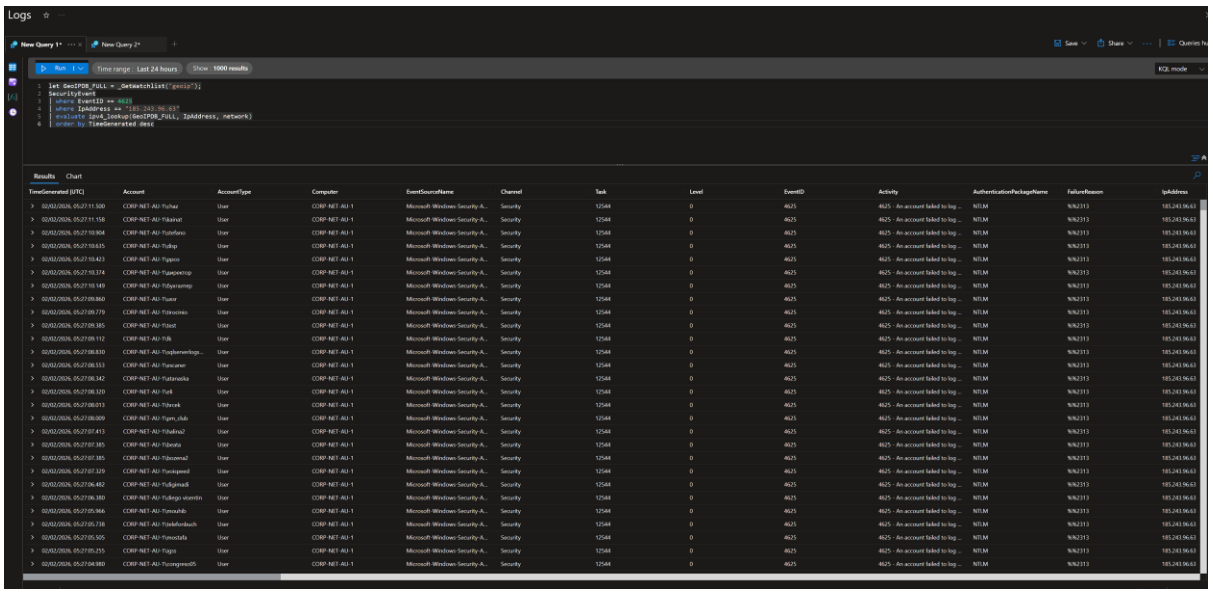

New Workbook
Done Editing
Advanced editor
Refresh
Auto refresh: Off
Editing: query - 0
Query Settings
Visual Formatting
Step Settings
Advanced Editor
Apply
Add a title
Press the Run Query button to see the data.
Done Editing
Cancel
Add

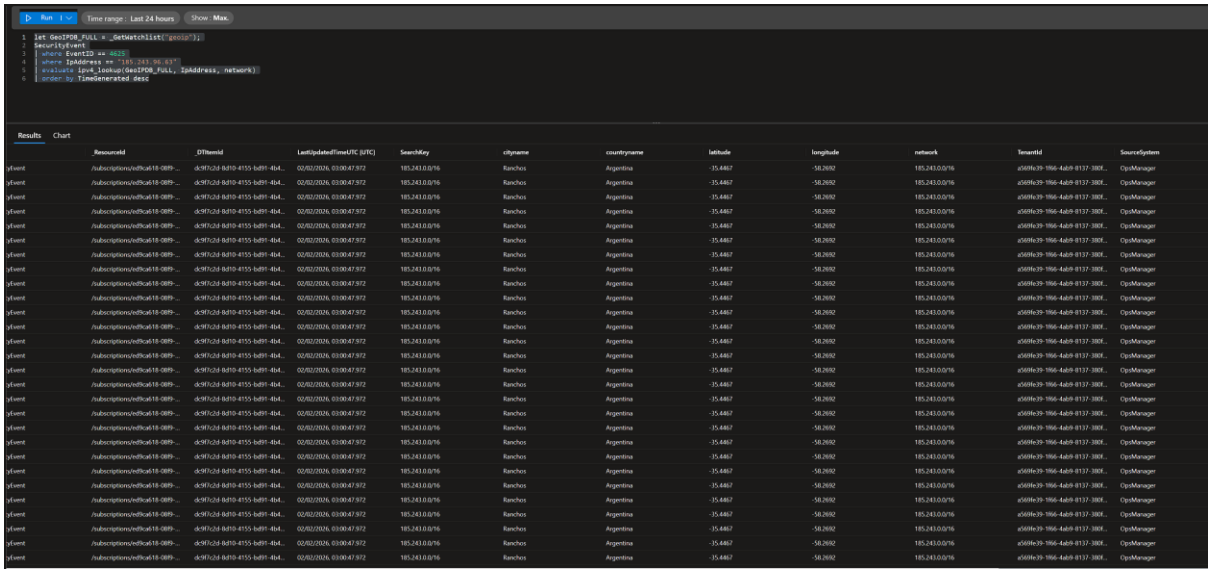

Results
Chart
TimeGenerated [UTC]
Account
AccountType
Computer
EventSourceName
Channel
Task
Level
EventData
EventID
Activity
AuthenticationPackageName

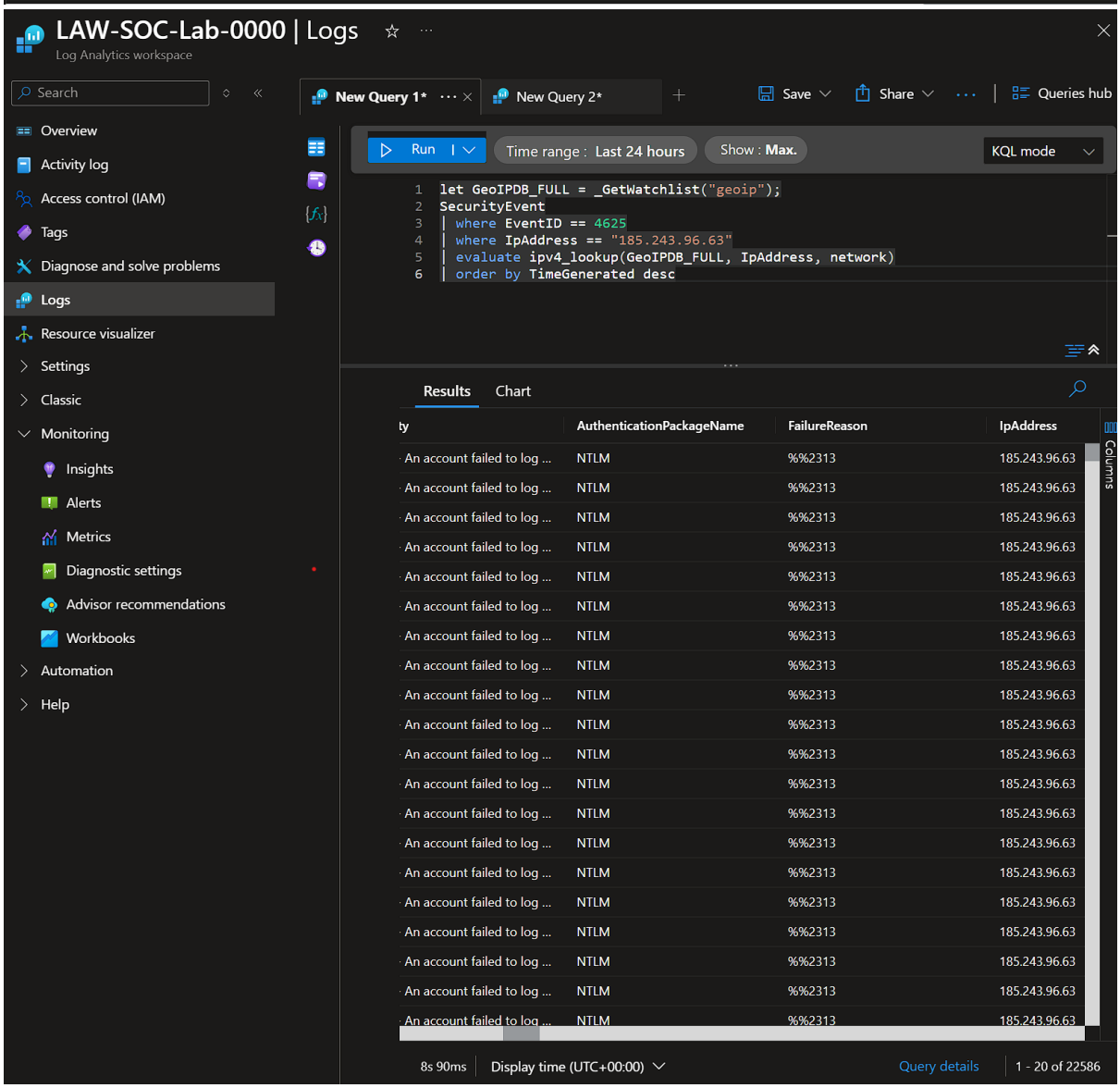

New Workbook
Done Editing
Advanced editor
Refresh
Auto refresh: Off
45.1 K
22.6 K
Add

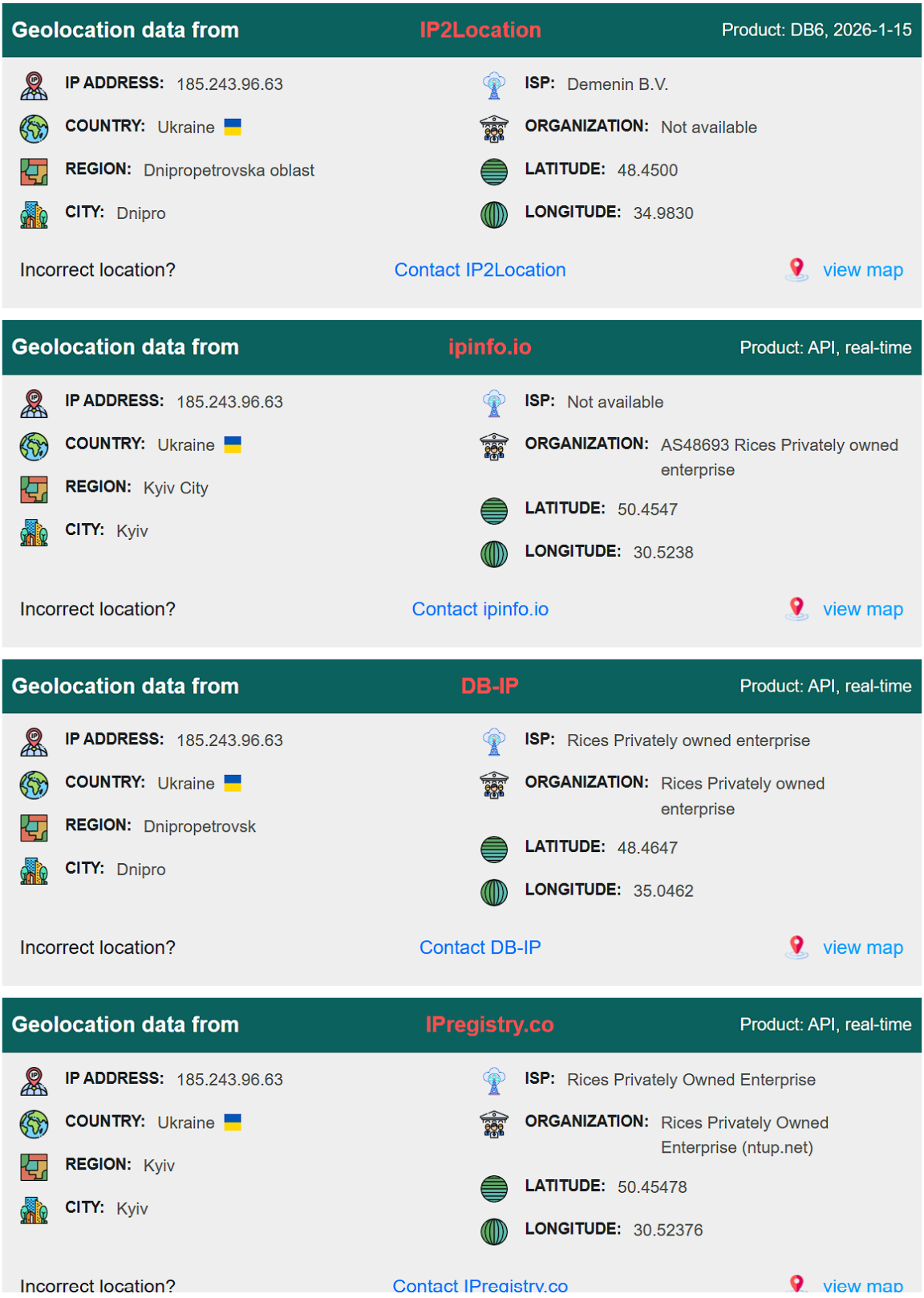

Save Workbook
Title *
Windows VM Attack Map
Location *
Australia Southeast
Save
Cancel




Logs
Run
Time range : Last 24 hours
Show : 1000 results
KQL mode
let GeoIPDB_FULL = _GetWatchlist("geoip");
SecurityEvent
| where EventID == 4625
| where IpAddress == "185.243.96.63"
| evaluate ipv4_lookup(GeoIPDB_FULL, IpAddress, network)
| order by TimeGenerated desc
Results
Chart




LAW-SOC-Lab-0000 | Logs
Log Analytics workspace
Search
New Query 1*
New Query 2*
Save
Share
Queries hub
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Logs
Resource visualizer
Settings
Classic
Monitoring
Insights
Alerts
Metrics
Diagnostic settings
Advisor recommendations
Workbooks
Automation
Help
Run
Time range : Last 24 hours
Show : Max.
KQL mode
let GeoIPDB_FULL = _GetWatchlist("geoip");
SecurityEvent
| where EventID == 4625
| where IpAddress == "185.243.96.63"
| evaluate ipv4_lookup(GeoIPDB_FULL, IpAddress, network)
| order by TimeGenerated desc
Results
Chart
ty
AuthenticationPackageName
FailureReason
IpAddress
An account failed to log ...
NTLM
%%2313
185.243.96.63
Columns
8s 90ms
Display time (UTC+00:00)
Query details
1 - 20 of 22586



Query: “let GeoIPDB_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.