SIEM Integration with Microsoft Sentinel: A Modern Approach

Author: Harshitkumar R. Panwala

Date: July 22, 2024

Documentation

Introduction

This project showcases the use of Microsoft Sentinel (previously known as Azure Sentinel) as a Security Information and Event Management (SIEM) tool to monitor and analyze failed Remote Desktop Protocol (RDP) attacks on a live virtual machine set up as a honeypot. By using a custom PowerShell script to parse Windows Event Logs for failed RDP attempts and leveraging a third-party API to gather geographic information about the attackers, the project visualizes the attack data on a map within Microsoft Sentinel.

Objectives

- **Real-Time Monitoring**: Track failed RDP attacks using Microsoft Sentinel.
- **Geolocation Extraction**: Use a custom PowerShell script and a geolocation API to identify the attackers' locations.
- **Data Visualization**: Display the geographic distribution of RDP attacks on a map.

Description

Key Features

- **Windows Event Logs Parsing**: Extract information about failed RDP logon attempts.
- **Geolocation Lookup**: Use the ipgeolocation.io API to convert attacker IP addresses into geographic locations.
- **Data Visualization**: Plot attacker locations on a map in Microsoft Sentinel.

Project Components

- **PowerShell Script**: Extracts failed RDP logon logs from the Windows Event Viewer.
- **Geolocation API**: Uses ipgeolocation.io to convert IP addresses into geographic locations.
- **Microsoft Sentinel Integration**: Ingests custom logs into Microsoft Sentinel and visualizes them on a map.

Setup and Usage

Prerequisites

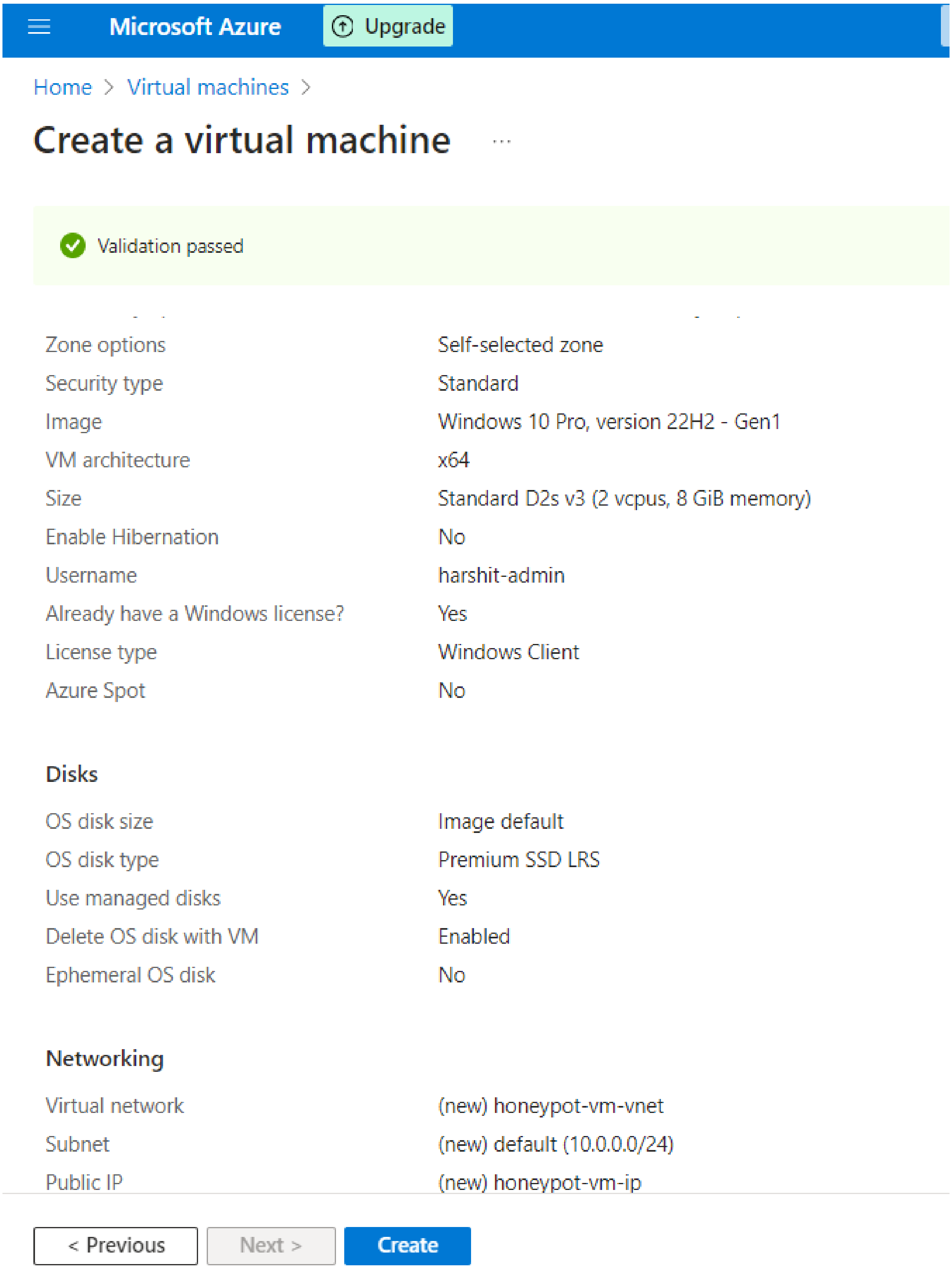
- An Azure subscription with Microsoft Sentinel enabled.
- A virtual machine configured as a honeypot with RDP enabled.
- PowerShell installed on the virtual machine.
- An API key from ipgeolocation.io.

Walkthrough

Step 1: Create a Virtual Machine in Azure

Create a VM with Network Configurations:

1. Log in to the Azure portal.
2. Navigate to "Virtual Machines" and select the option to create a new VM.
3. During the setup, configure the network settings to allow connections on all ports, temporarily disabling any security restrictions.
4. Deploy a virtual machine with RDP enabled to act as a honeypot.
5. Ensure the machine logs RDP events by configuring the security policies.



Create a virtual machine

Validation passed

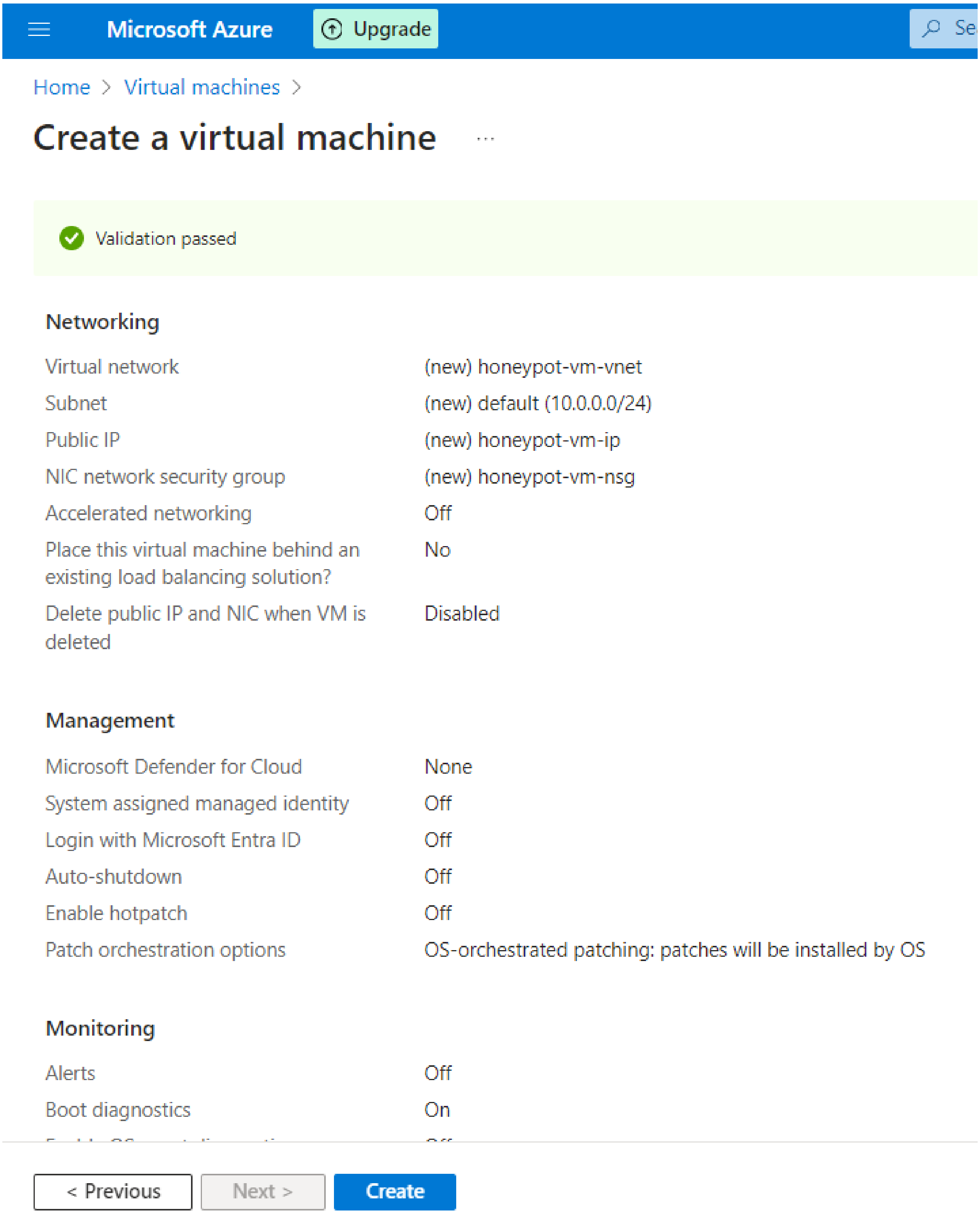
Zone options	Self-selected zone
Security type	Standard
Image	Windows 10 Pro, version 22H2 - Gen1
VM architecture	x64
Size	Standard D2s v3 (2 vcpus, 8 GiB memory)
Enable Hibernation	No
Username	harshit-admin
Already have a Windows license?	Yes
License type	Windows Client
Azure Spot	No

Disks

OS disk size	Image default
OS disk type	Premium SSD LRS
Use managed disks	Yes
Delete OS disk with VM	Enabled
Ephemeral OS disk	No

Networking

Virtual network	(new) honeypot-vm-vnet
Subnet	(new) default (10.0.0.0/24)
Public IP	(new) honeypot-vm-ip



Home > Virtual machines >

Create a virtual machine

✓ Validation passed

Networking

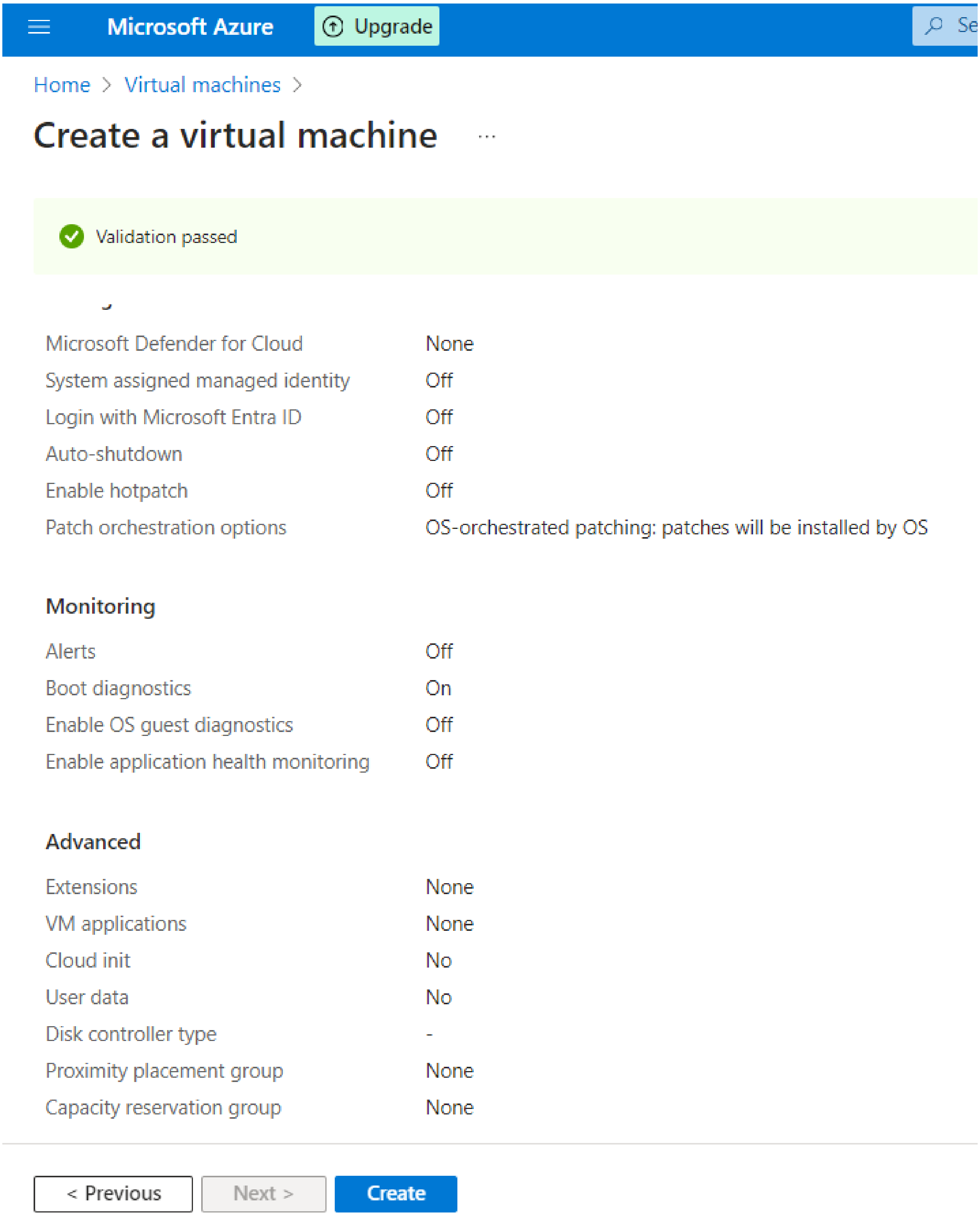
Virtual network	(new) honeypot-vm-vnet
Subnet	(new) default (10.0.0.0/24)
Public IP	(new) honeypot-vm-ip
NIC network security group	(new) honeypot-vm-nsg
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No
Delete public IP and NIC when VM is deleted	Disabled

Management

Microsoft Defender for Cloud	None
System assigned managed identity	Off
Login with Microsoft Entra ID	Off
Auto-shutdown	Off
Enable hotpatch	Off
Patch orchestration options	OS-orchestrated patching: patches will be installed by OS

Monitoring

Alerts	Off
Boot diagnostics	On



Create a virtual machine

✓ Validation passed

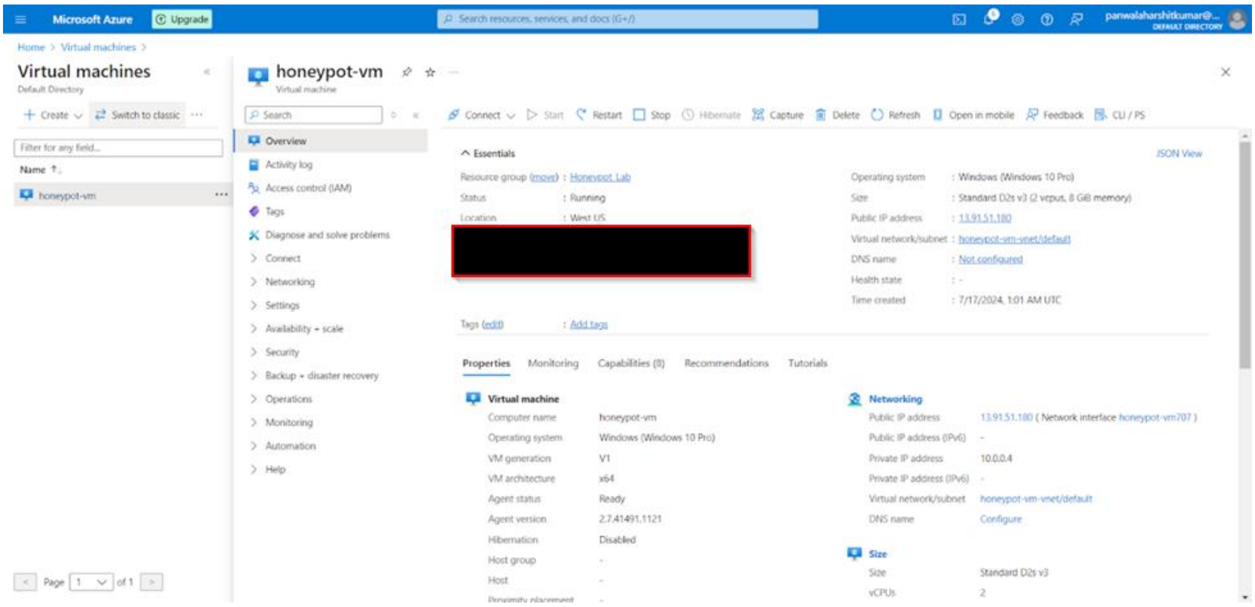
Microsoft Defender for Cloud	None
System assigned managed identity	Off
Login with Microsoft Entra ID	Off
Auto-shutdown	Off
Enable hotpatch	Off
Patch orchestration options	OS-orchestrated patching: patches will be installed by OS

Monitoring

Alerts	Off
Boot diagnostics	On
Enable OS guest diagnostics	Off
Enable application health monitoring	Off

Advanced

Extensions	None
VM applications	None
Cloud init	No
User data	No
Disk controller type	-
Proximity placement group	None
Capacity reservation group	None



Essentials

Resource group (move) : Honeypot_Lab
Status : Running
Location : West US

[redacted]

Tags (edit) : Add tags

Operating system : Windows (Windows 10 Pro)
Size : Standard D2s v3 (2 vcpus, 8 GiB memory)
Public IP address : 13.91.51.180
Virtual network/subnet : honeypot-vm-vnet/default
DNS name : Not configured
Health state : -
Time created : 7/17/2024, 1:01 AM UTC

Virtual machine

Computer name	honeypot-vm
Operating system	Windows (Windows 10 Pro)
VM generation	V1
VM architecture	x64
Agent status	Ready
Agent version	2.7.41491.1121
Hibernation	Disabled
Host group	-
Host	-
Proximity placement	-

Networking

Public IP address	13.91.51.180 (Network interface honeypot-vm707)
Public IP address (IPv6)	-
Private IP address	10.0.0.4
Private IP address (IPv6)	-
Virtual network/subnet	honeypot-vm-vnet/default
DNS name	Configure

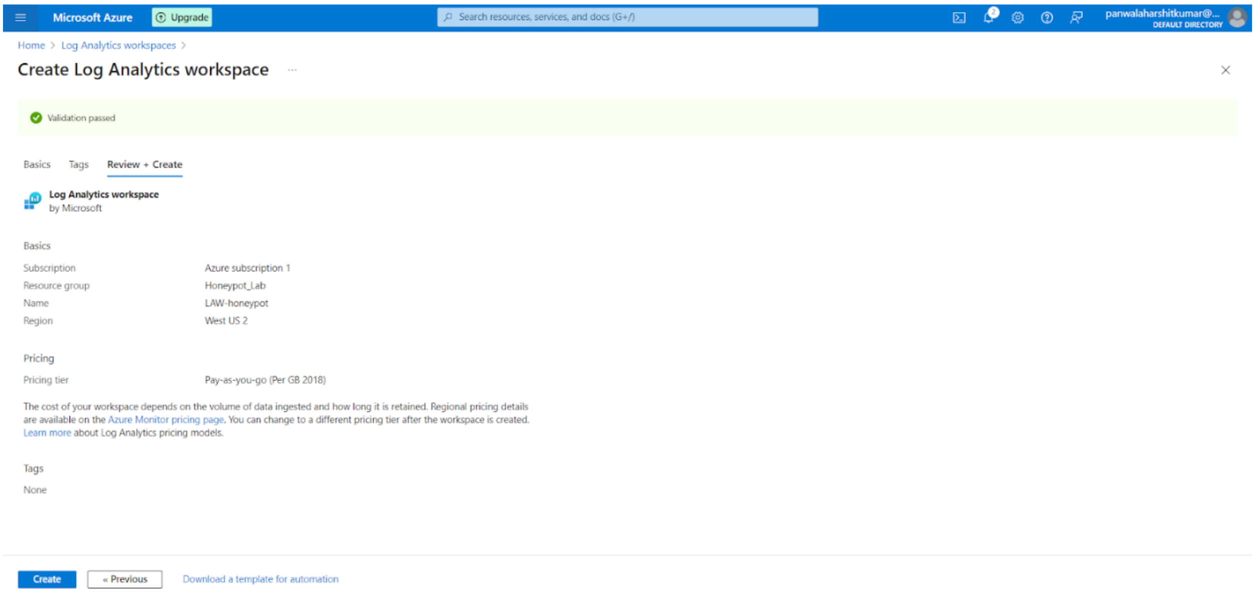
Size

Size	Standard D2s v3
vCPUs	2

Step 2: Create a Log Analytics Workspace

Set Up a Log Analytics Workspace:

1. In the Azure portal, search for "Log Analytics Workspaces".
2. Follow the prompts to create a new workspace that will be used to collect and analyze log data from your VM.


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
panwalaharshitkumar@...
DEFAULT DIRECTORY
Home > Log Analytics workspaces >
Create Log Analytics workspace
Basics
Tags
Review + Create
Create
« Previous
Download a template for automation

Validation passed

Log Analytics workspace
by Microsoft

Basics

Subscription	Azure subscription 1
Resource group	Honeypot_Lab
Name	LAW-honeypot
Region	West US 2

Pricing

Pricing tier	Pay-as-you-go (Per GB 2018)

The cost of your workspace depends on the volume of data ingested and how long it is retained. Regional pricing details are available on the Azure Monitor pricing page. You can change to a different pricing tier after the workspace is created. Learn more about Log Analytics pricing models.

Tags

None

Step 3: Configure Microsoft Defender for Cloud

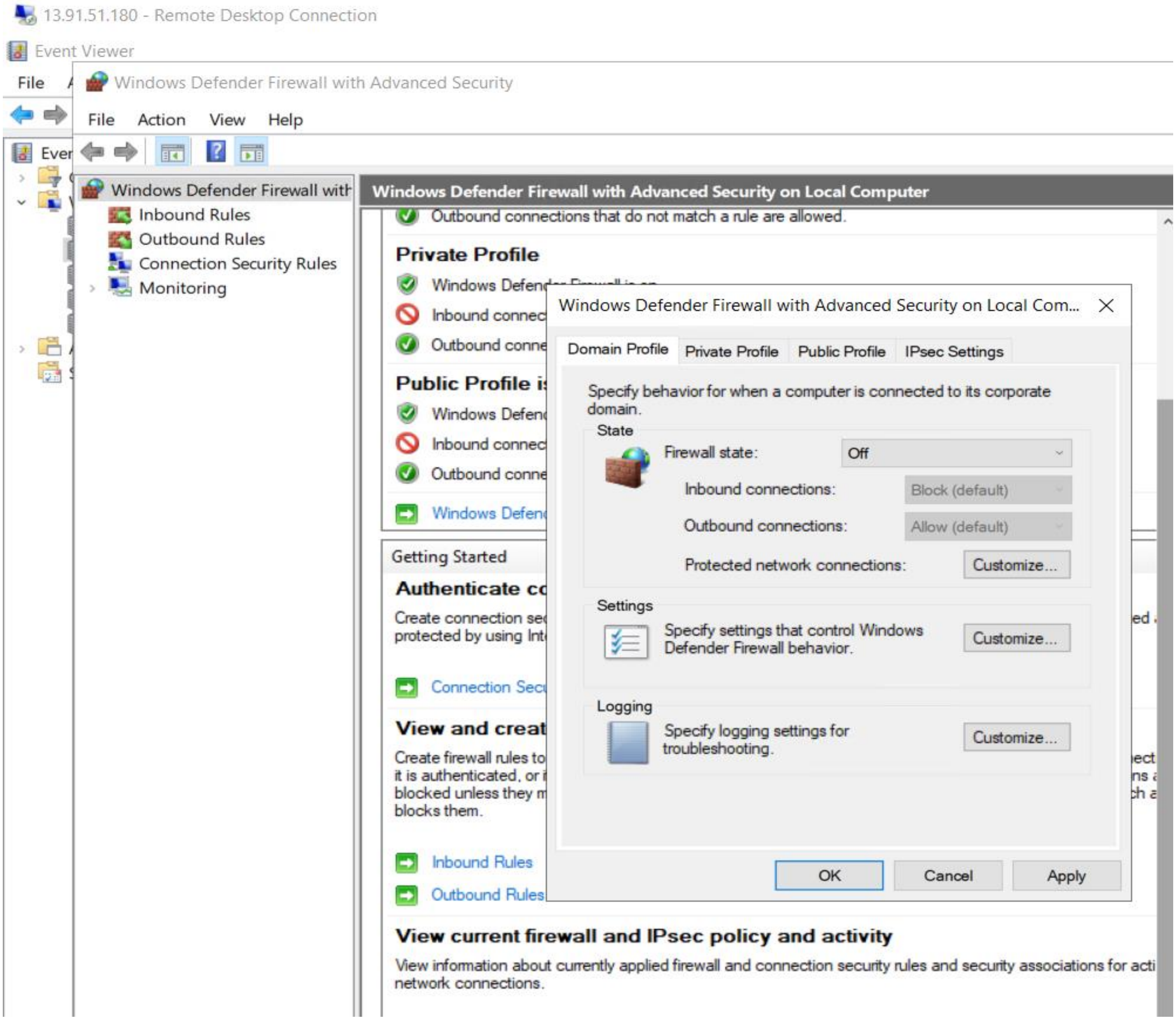
Enable Microsoft Defender for Servers:

1. In the Azure portal, navigate to "Microsoft Defender for Cloud".
2. Enable Microsoft Defender specifically for the VM, focusing on server protection. For simplicity, you can disable other protections.

Step 4: Configure the VM Firewall

Access the VM via Remote Desktop:

1. Use Remote Desktop Connection to log in to the VM.
2. Open the Windows Firewall settings (wf.msc) and turn off firewall protection for all profiles (private, public, domain).
3. Ensure the VM can be pinged from your machine to maintain connectivity.



13.91.51.180 - Remote Desktop Connection

Windows Defender Firewall with Advanced Security on Local Computer

Outbound connections that do not match a rule are allowed.

Windows Defender Firewall with Advanced Security on Local Com...

Domain Profile | Private Profile | Public Profile | IPsec Settings

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: Off

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections: Customize...

Settings

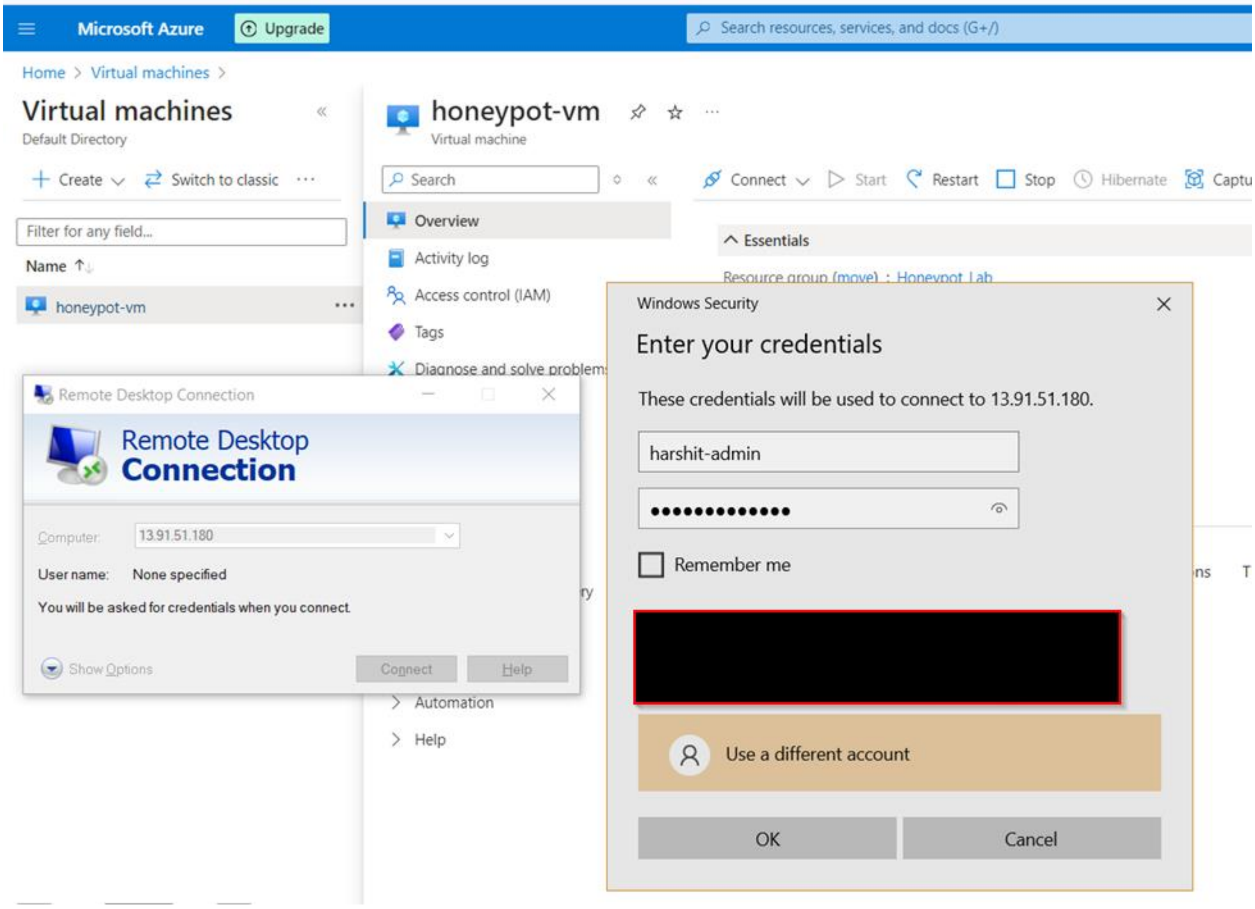
Specify settings that control Windows Defender Firewall behavior. Customize...

Logging

Specify logging settings for troubleshooting. Customize...

View current firewall and IPsec policy and activity

View information about currently applied firewall and connection security rules and security associations for acti network connections.



Remote Desktop Connection

Computer: 13.91.51.180

User name: None specified

You will be asked for credentials when you connect.

Windows Security

Enter your credentials

These credentials will be used to connect to 13.91.51.180.

harshit-admin

••••••••••••••

□ Remember me

[redacted]

Use a different account

OK | Cancel

Step 5: Enable Microsoft Sentinel

Set Up Microsoft Sentinel:

1. Navigate to "Microsoft Sentinel" in the Azure portal.
2. Add a new Sentinel workspace and link it to the Log Analytics Workspace you created earlier.

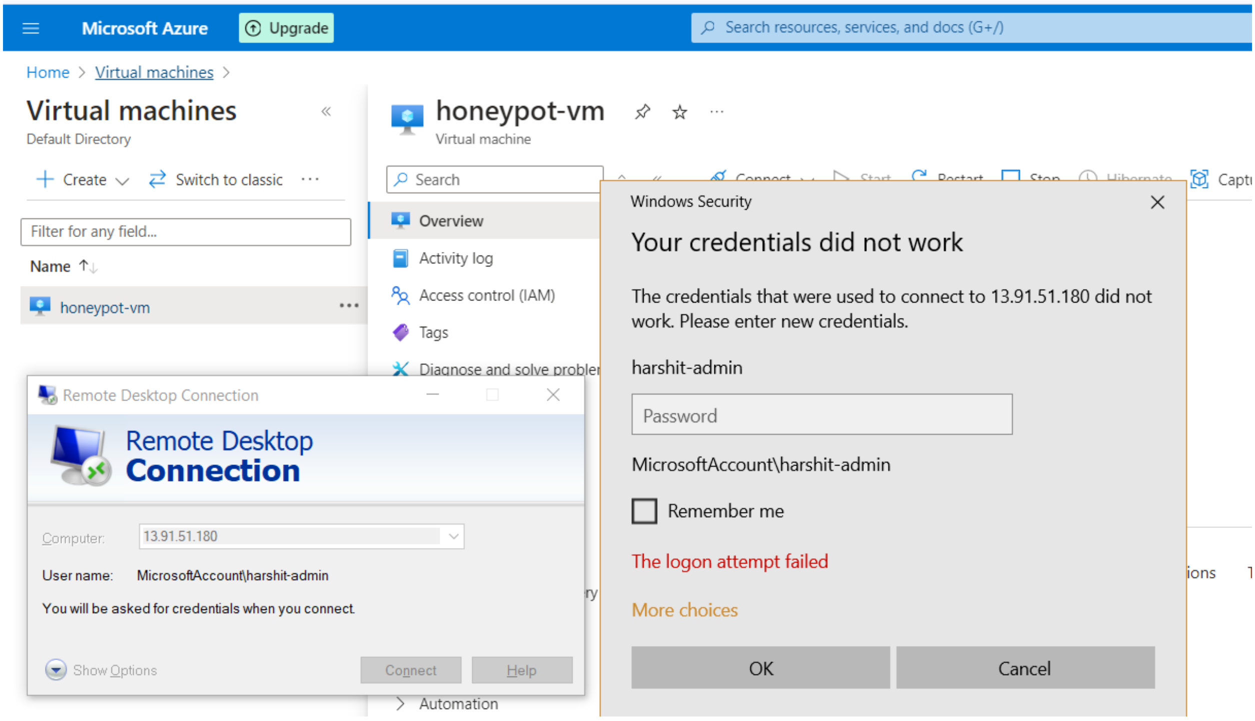
Connect the Virtual Machine to Microsoft Sentinel:

1. In the Sentinel workspace, go to "Data connectors".
2. Select "Windows Security Events" and follow the instructions to connect to the virtual machine.

Step 6: Verify Event Logging

Check Event Logs in Event Viewer:

1. Open the Event Viewer on the VM.
2. Attempt a failed login via Remote Desktop to ensure the event is logged.
3. Verify that the event log captures the IP address of the machine making the attempt.



Remote Desktop Connection

Computer: 13.91.51.180

User name: MicrosoftAccount\harshit-admin

You will be asked for credentials when you connect.

Your credentials did not work

The credentials that were used to connect to 13.91.51.180 did not work. Please enter new credentials.

harshit-admin

Password

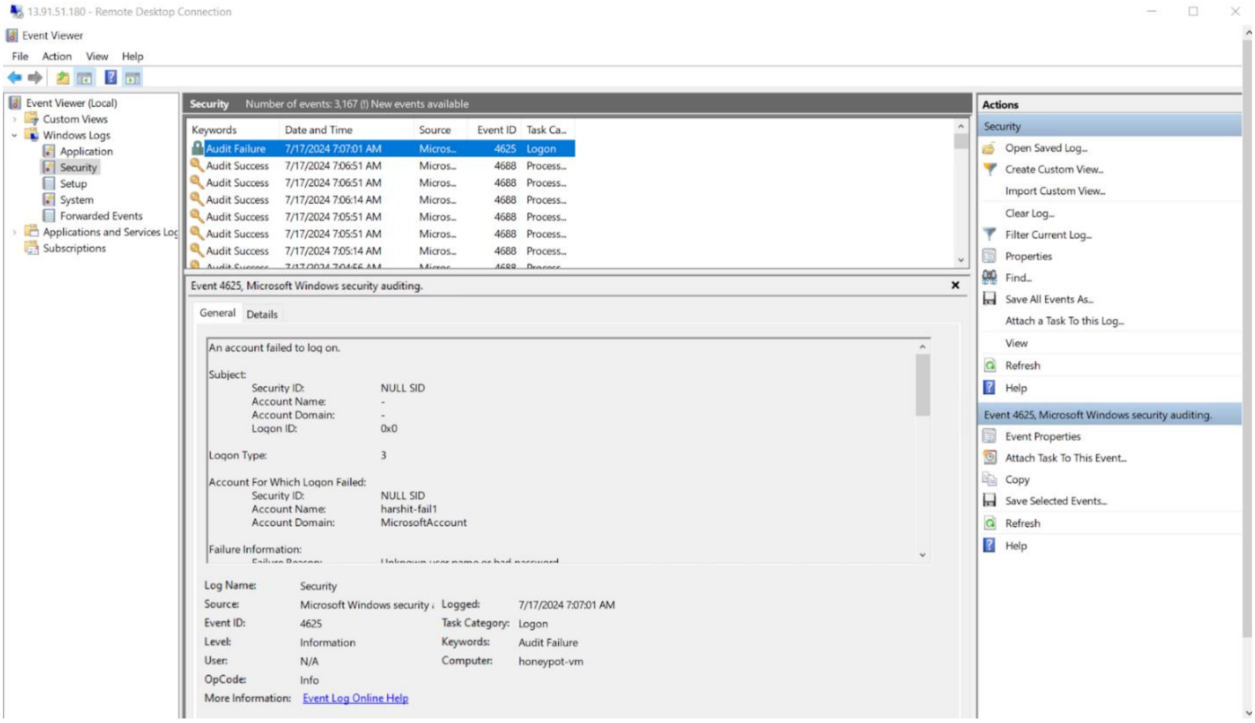
MicrosoftAccount\harshit-admin

□ Remember me

The logon attempt failed

More choices

OK Cancel



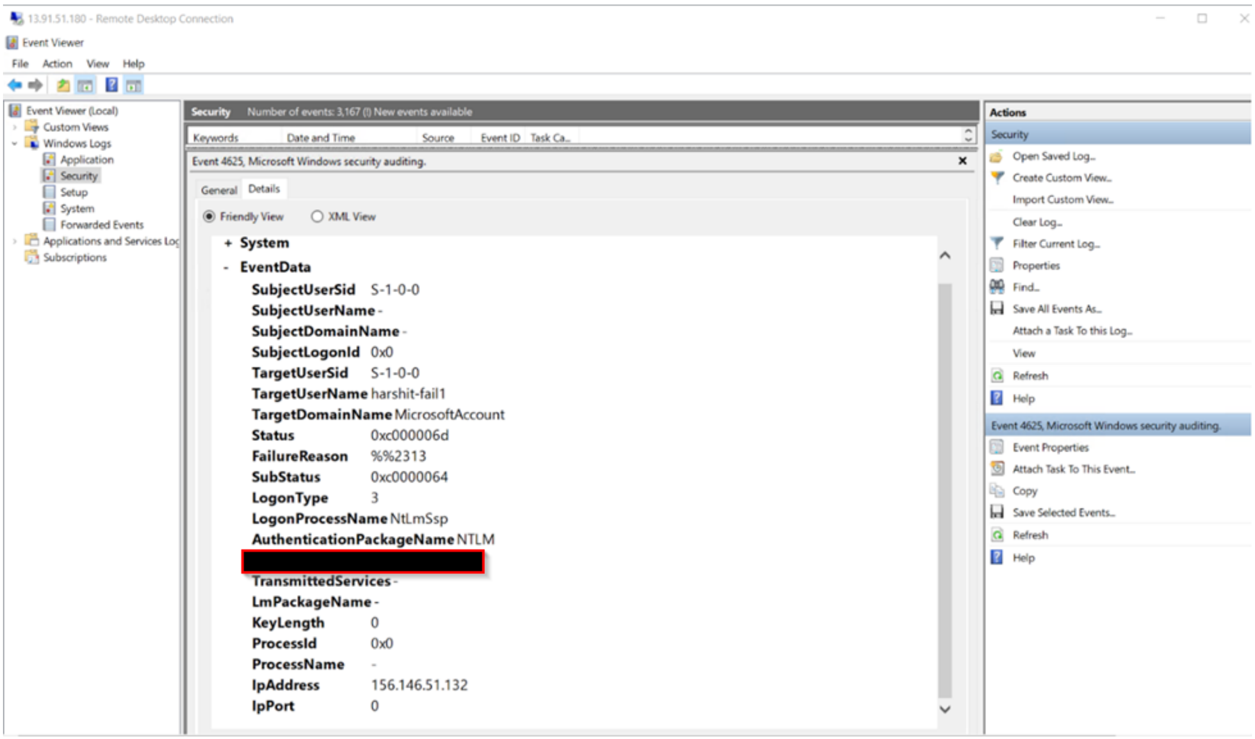
Security Number of events: 3,167 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Ca...
Audit Failure	7/17/2024 7:07:01 AM	Micros...	4625	Logon
Audit Success	7/17/2024 7:06:51 AM	Micros...	4688	Process...
Audit Success	7/17/2024 7:06:51 AM	Micros...	4688	Process...
Audit Success	7/17/2024 7:06:14 AM	Micros...	4688	Process...
Audit Success	7/17/2024 7:05:51 AM	Micros...	4688	Process...
Audit Success	7/17/2024 7:05:51 AM	Micros...	4688	Process...
Audit Success	7/17/2024 7:05:14 AM	Micros...	4688	Process...
Audit Success	7/17/2024 7:04:56 AM	Micros...	4688	Process...

Event 4625, Microsoft Windows security auditing.

```
An account failed to log on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           harshit-fail1
        Account Domain:         MicrosoftAccount

Failure Information:
        Failure Reason:         Unknown user name or bad password
```

```
Log Name:          Security
Source:            Microsoft Windows security ;  Logged:          7/17/2024 7:07:01 AM
Event ID:          4625                          Task Category:   Logon
Level:             Information                   Keywords:        Audit Failure
User:              N/A                           Computer:        honeypot-vm
OpCode:            Info
More Information:  Event Log Online Help
```



Event 4625, Microsoft Windows security auditing.

● Friendly View ○ XML View

+ System

- EventData

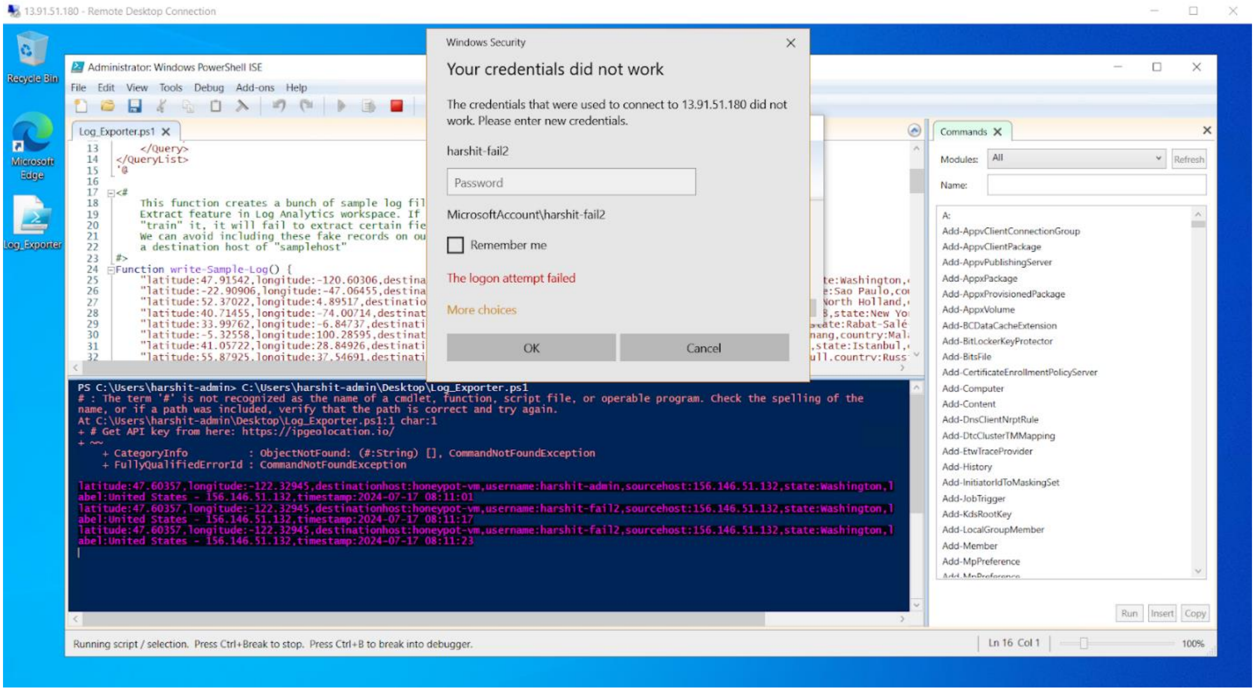
SubjectUserSid	S-1-0-0
SubjectUserName	-
SubjectDomainName	-
SubjectLogonId	0x0
TargetUserSid	S-1-0-0
TargetUserName	harshit-fail1
TargetDomainName	MicrosoftAccount
Status	0xc000006d
FailureReason	%%2313
SubStatus	0xc0000064
LogonType	3
LogonProcessName	NtLmSsp
AuthenticationPackageName	NTLM
[redacted]	
TransmittedServices	-
LmPackageName	-
KeyLength	0
ProcessId	0x0
ProcessName	-
IpAddress	156.146.51.132
IpPort	0

Step 7: Execute the PowerShell Script

Update the Script with Your API Key: Log_Exporter.ps1

Run the PowerShell Script:

1. Update the script with your ipgeolocation.io API key.
2. Execute the script to parse event logs and log geographic data.



Windows Security

Your credentials did not work

The credentials that were used to connect to 13.91.51.180 did not work. Please enter new credentials.

harshit-fail2

Password

MicrosoftAccount\harshit-fail2

□ Remember me

The logon attempt failed

More choices

OK Cancel

```
    </Query>
</QueryList>
'@

<#
    This function creates a bunch of sample log fil
    Extract feature in Log Analytics workspace. If
    "train" it, it will fail to extract certain fie
    We can avoid including these fake records on ou
    a destination host of "samplehost"
#>
Function write-Sample-Log() {
    "latitude:47.91542,longitude:-120.60306,destina
    "latitude:-22.90906,longitude:-47.06455,destina
    "latitude:52.37022,longitude:4.89517,destinatio
    "latitude:40.71455,longitude:-74.00714,destinat
    "latitude:33.99762,longitude:-6.84737,destinati
    "latitude:-5.32558,longitude:100.28595,destinat
    "latitude:41.05722,longitude:28.84926,destinati
    "latitude:55.87925,longitude:37.54691,destinati
```

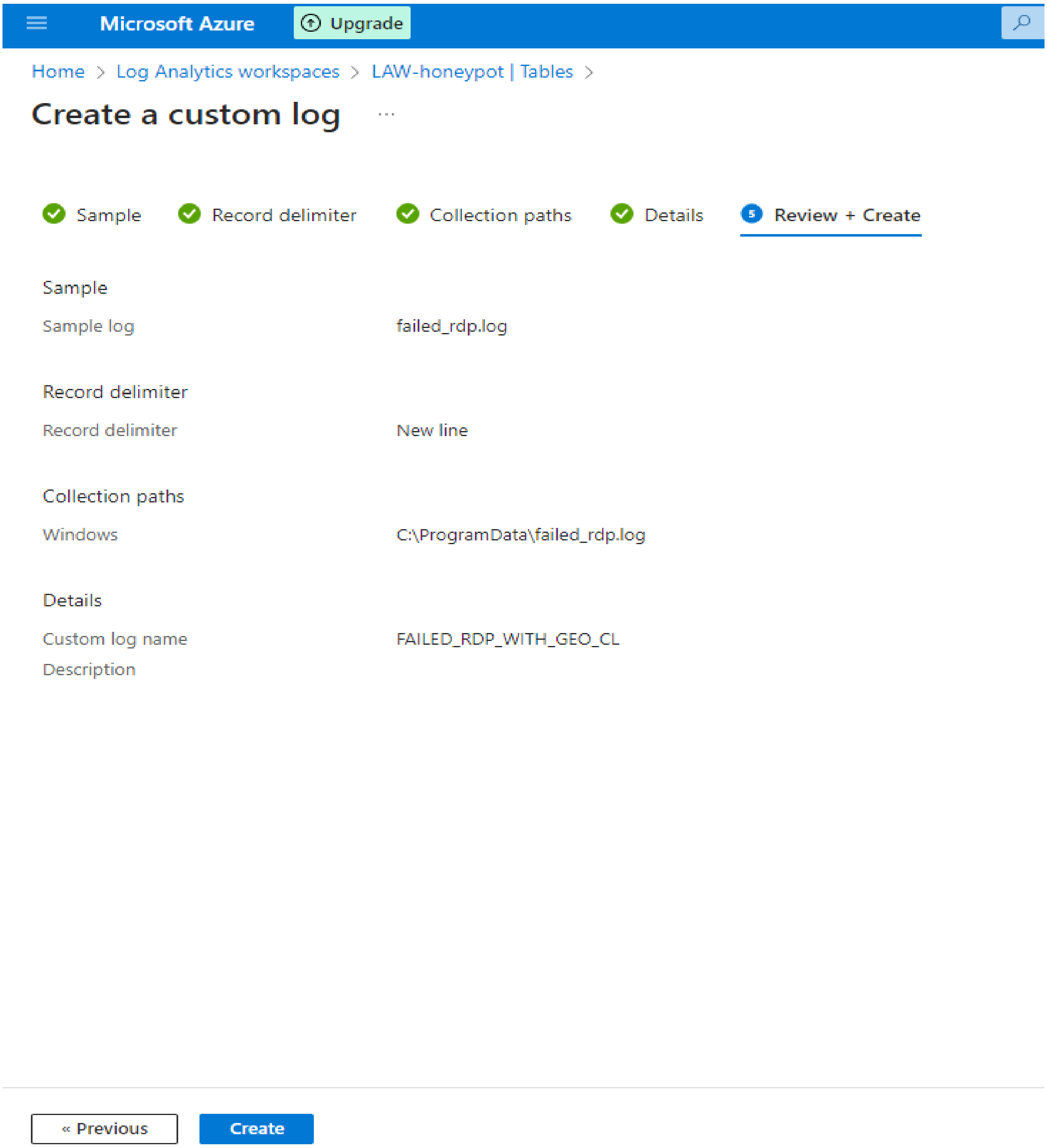
```
PS C:\Users\harshit-admin> C:\Users\harshit-admin\Desktop\Log_Exporter.ps1
# : The term '#' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the
name, or if a path was included, verify that the path is correct and try again.
At C:\Users\harshit-admin\Desktop\Log_Exporter.ps1:1 char:1
+ # Get API key from here: https://ipgeolocation.io/
+ ~~
    + CategoryInfo          : ObjectNotFound: (#:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException

latitude:47.60357,longitude:-122.32945,destinationhost:honeypot-vm,username:harshit-admin,sourcehost:156.146.51.132,state:Washington,l
abel:United States - 156.146.51.132,timestamp:2024-07-17 08:11:01
latitude:47.60357,longitude:-122.32945,destinationhost:honeypot-vm,username:harshit-fail2,sourcehost:156.146.51.132,state:Washington,l
abel:United States - 156.146.51.132,timestamp:2024-07-17 08:11:17
latitude:47.60357,longitude:-122.32945,destinationhost:honeypot-vm,username:harshit-fail2,sourcehost:156.146.51.132,state:Washington,l
abel:United States - 156.146.51.132,timestamp:2024-07-17 08:11:23
```

Running script / selection. Press Ctrl+Break to stop. Press Ctrl+B to break into debugger.

Step 8: Ingest Custom Logs into Microsoft Sentinel

Configure Custom Log Ingestion:

1. In the Sentinel workspace, go to "Custom Logs".
2. Add a new custom log source pointing to the log files generated by the PowerShell script.
3. Observe the failed attempts in the file: failed_rdp.log



Sample

Sample log	failed_rdp.log

Record delimiter

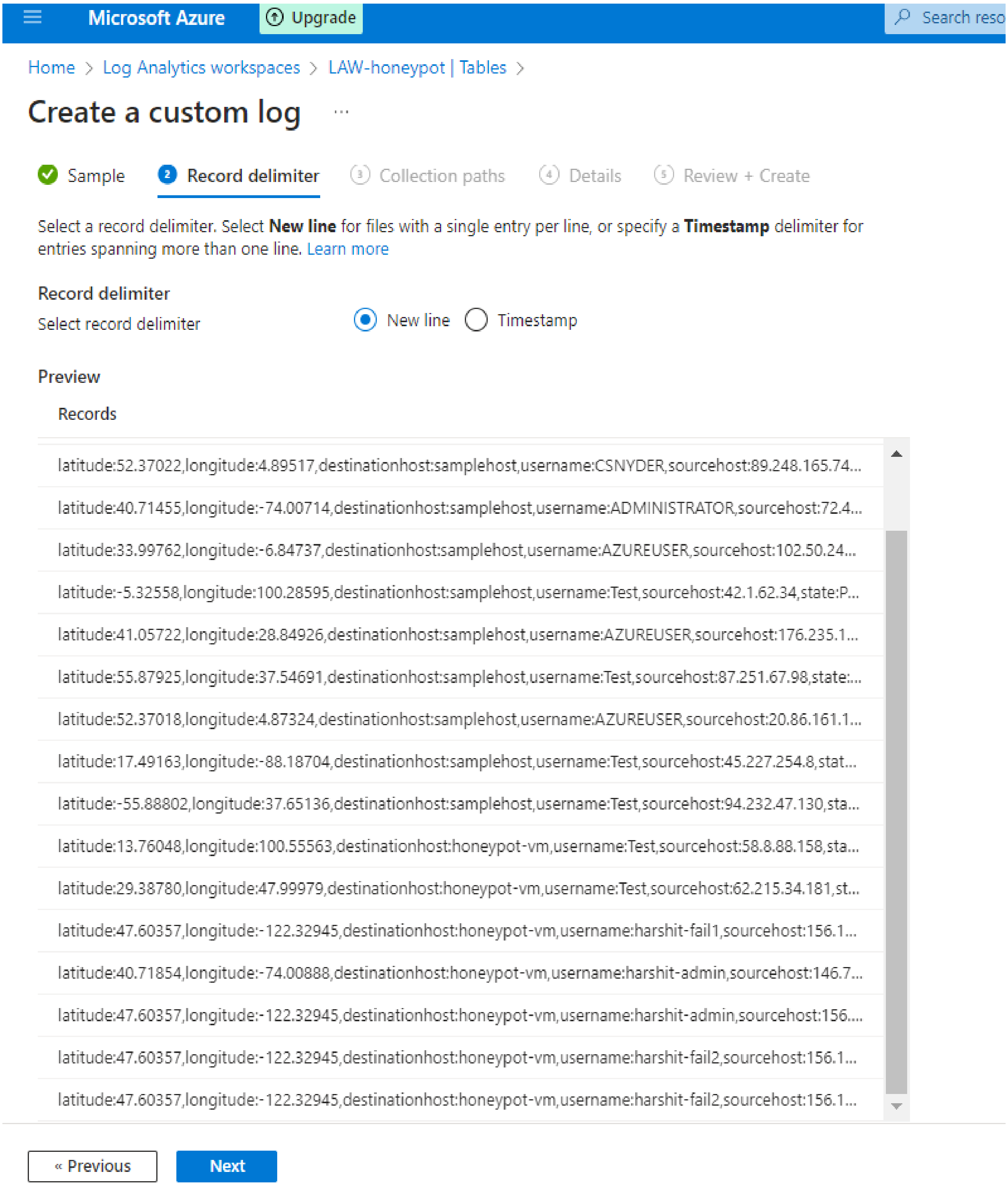
Record delimiter	New line

Collection paths

Windows	C:\ProgramData\failed_rdp.log

Details

Custom log name	FAILED_RDP_WITH_GEO_CL
Description	



Create a custom log

Select a record delimiter. Select **New line** for files with a single entry per line, or specify a **Timestamp** delimiter for entries spanning more than one line. Learn more

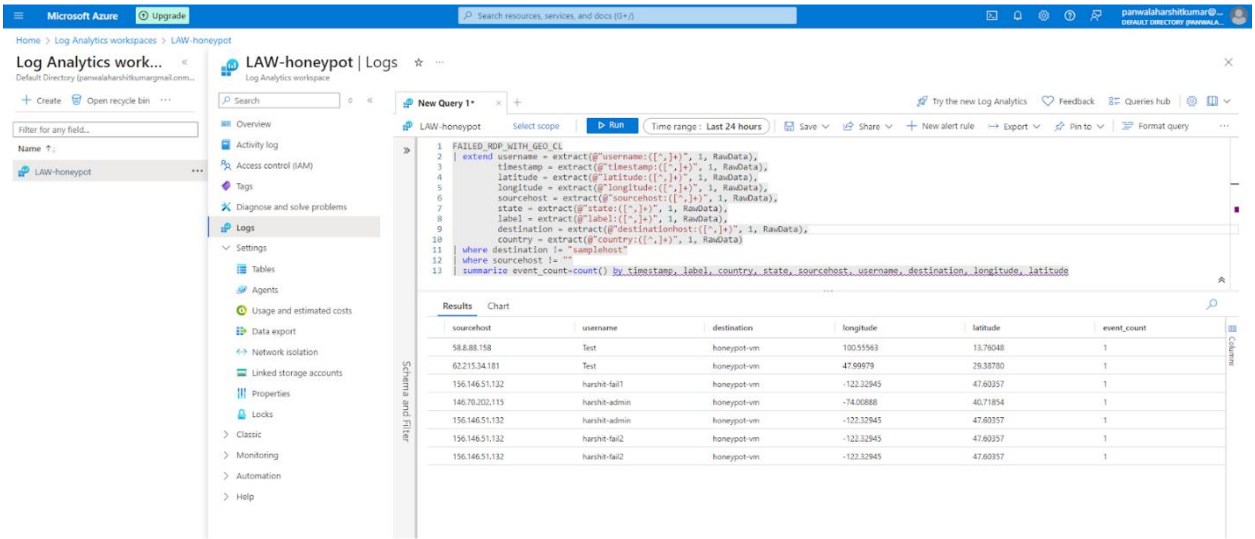
Record delimiter

Select record delimiter ● New line ○ Timestamp

Preview

Records

```
latitude:52.37022,longitude:4.89517,destinationhost:samplehost,username:CSNYDER,sourcehost:89.248.165.74...
latitude:40.71455,longitude:-74.00714,destinationhost:samplehost,username:ADMINISTRATOR,sourcehost:72.4...
latitude:33.99762,longitude:-6.84737,destinationhost:samplehost,username:AZUREUSER,sourcehost:102.50.24...
latitude:-5.32558,longitude:100.28595,destinationhost:samplehost,username:Test,sourcehost:42.1.62.34,state:P...
latitude:41.05722,longitude:28.84926,destinationhost:samplehost,username:AZUREUSER,sourcehost:176.235.1...
latitude:55.87925,longitude:37.54691,destinationhost:samplehost,username:Test,sourcehost:87.251.67.98,state:...
latitude:52.37018,longitude:4.87324,destinationhost:samplehost,username:AZUREUSER,sourcehost:20.86.161.1...
latitude:17.49163,longitude:-88.18704,destinationhost:samplehost,username:Test,sourcehost:45.227.254.8,stat...
latitude:-55.88802,longitude:37.65136,destinationhost:samplehost,username:Test,sourcehost:94.232.47.130,sta...
latitude:13.76048,longitude:100.55563,destinationhost:honeypot-vm,username:Test,sourcehost:58.8.88.158,sta...
latitude:29.38780,longitude:47.99979,destinationhost:honeypot-vm,username:Test,sourcehost:62.215.34.181,st...
latitude:47.60357,longitude:-122.32945,destinationhost:honeypot-vm,username:harshit-fail1,sourcehost:156.1...
latitude:40.71854,longitude:-74.00888,destinationhost:honeypot-vm,username:harshit-admin,sourcehost:146.7...
latitude:47.60357,longitude:-122.32945,destinationhost:honeypot-vm,username:harshit-admin,sourcehost:156....
latitude:47.60357,longitude:-122.32945,destinationhost:honeypot-vm,username:harshit-fail2,sourcehost:156.1...
latitude:47.60357,longitude:-122.32945,destinationhost:honeypot-vm,username:harshit-fail2,sourcehost:156.1...
```



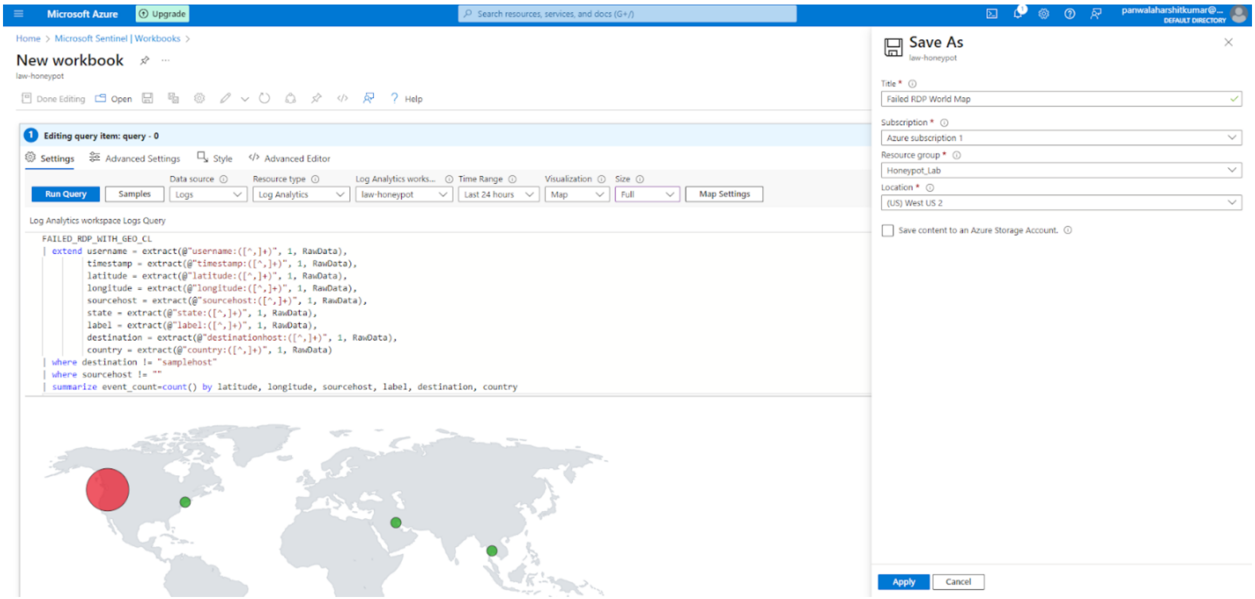
```
FAILED_RDP_WITH_GEO_CL
| extend username = extract(@"username:([^,]+)", 1, RawData),
         timestamp = extract(@"timestamp:([^,]+)", 1, RawData),
         latitude = extract(@"latitude:([^,]+)", 1, RawData),
         longitude = extract(@"longitude:([^,]+)", 1, RawData),
         sourcehost = 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, sourcehost, username, destination, longitude, latitude
```

sourcehost	username	destination	longitude	latitude	event_count
58.8.88.158	Test	honeypot-vm	100.55563	13.76048	1
62.215.34.181	Test	honeypot-vm	47.99979	29.38780	1
156.146.51.132	harshit-fail1	honeypot-vm	-122.32945	47.60357	1
146.70.202.115	harshit-admin	honeypot-vm	-74.00888	40.71854	1
156.146.51.132	harshit-admin	honeypot-vm	-122.32945	47.60357	1
156.146.51.132	harshit-fail2	honeypot-vm	-122.32945	47.60357	1
156.146.51.132	harshit-fail2	honeypot-vm	-122.32945	47.60357	1

Step 9: Visualize Data in Microsoft Sentinel

Create Map Visualization:

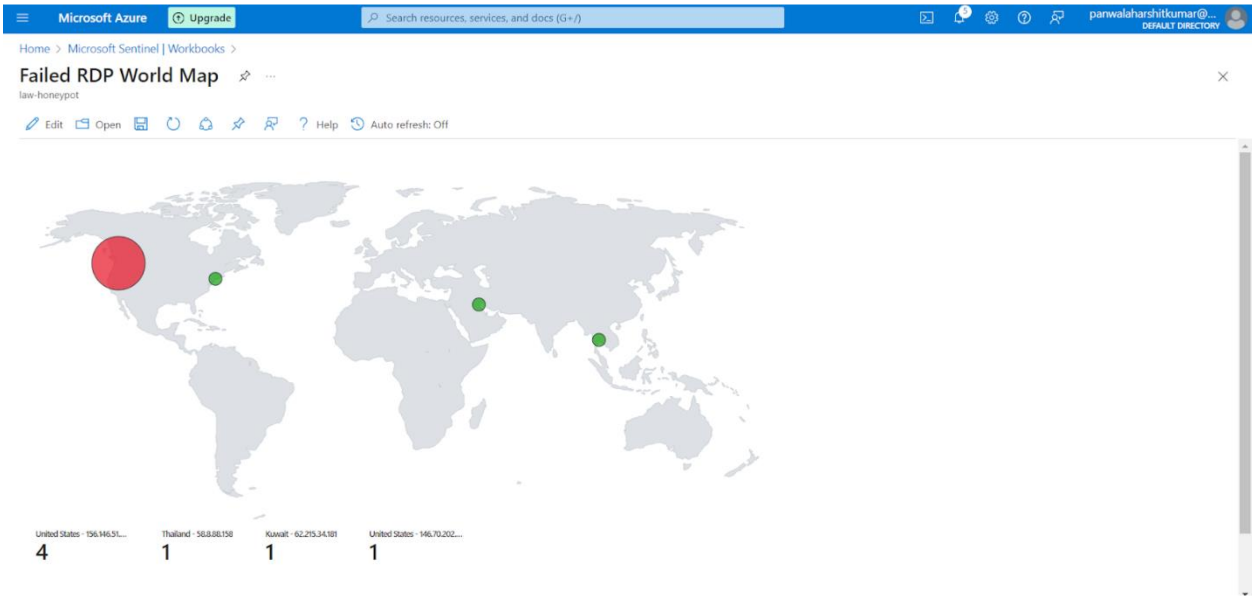
1. Use Microsoft Sentinel's built-in map visualization tool to plot the geolocation data of failed RDP attempts.
2. This will provide a visual representation of where the attacks are originating from, helping you to better understand and respond to potential threats.



Data source: Logs
Resource type: Log Analytics
Log Analytics works...: law-honeypot
Time Range: Last 24 hours
Visualization: Map
Size: Full

```
FAILED_RDP_WITH_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 latitude, longitude, sourcehost, label, destination, country
```

Title *: Failed RDP World Map
Subscription *: Azure subscription 1
Resource group *: Honeypot_Lab
Location *: (US) West US 2
□ Save content to an Azure Storage Account.

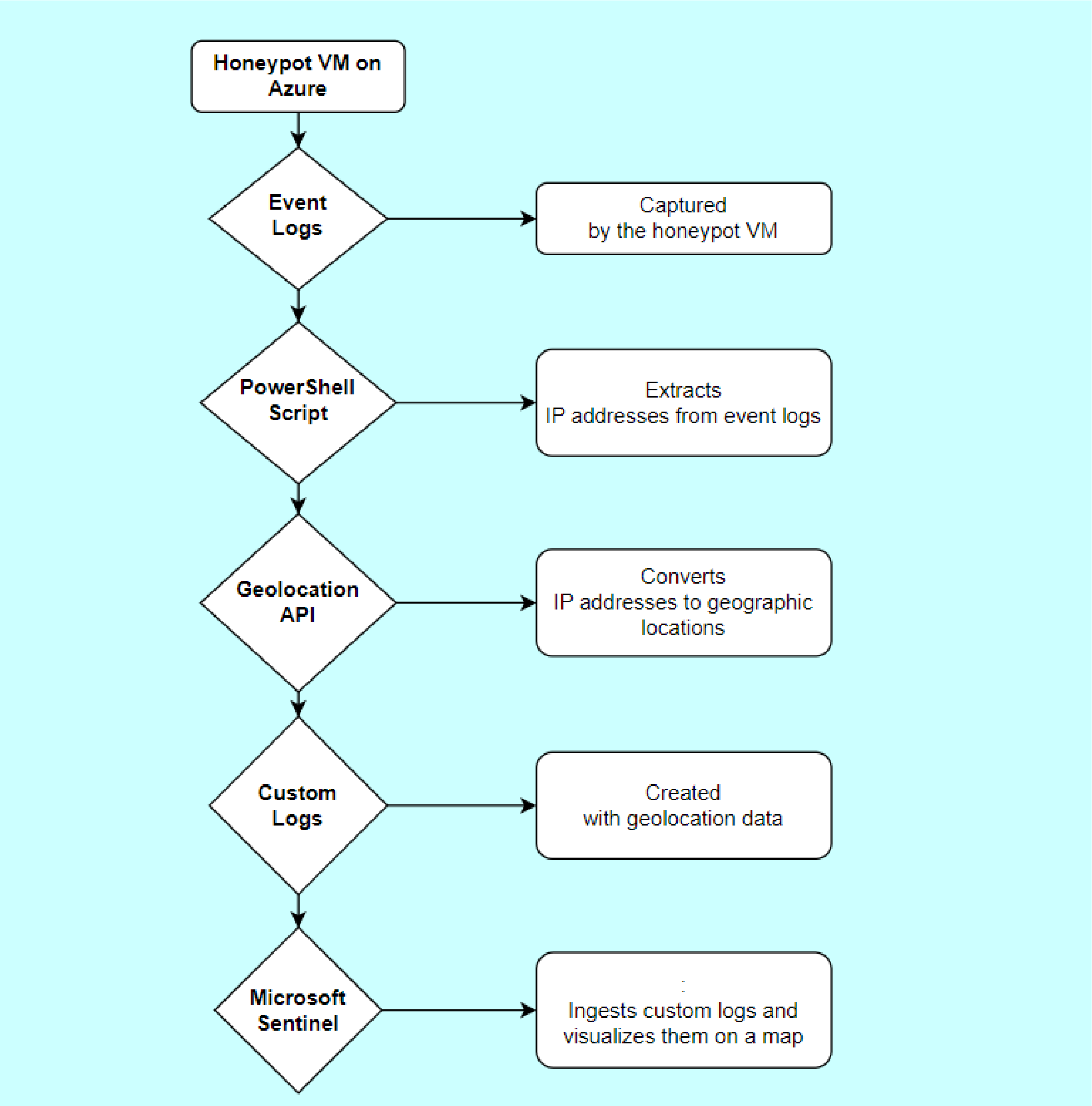


United States - 156.146.51...	Thailand - 58.8.88.158	Kuwait - 62.215.34.181	United States - 146.70.202...
4	1	1	1

Analysis and Visualization

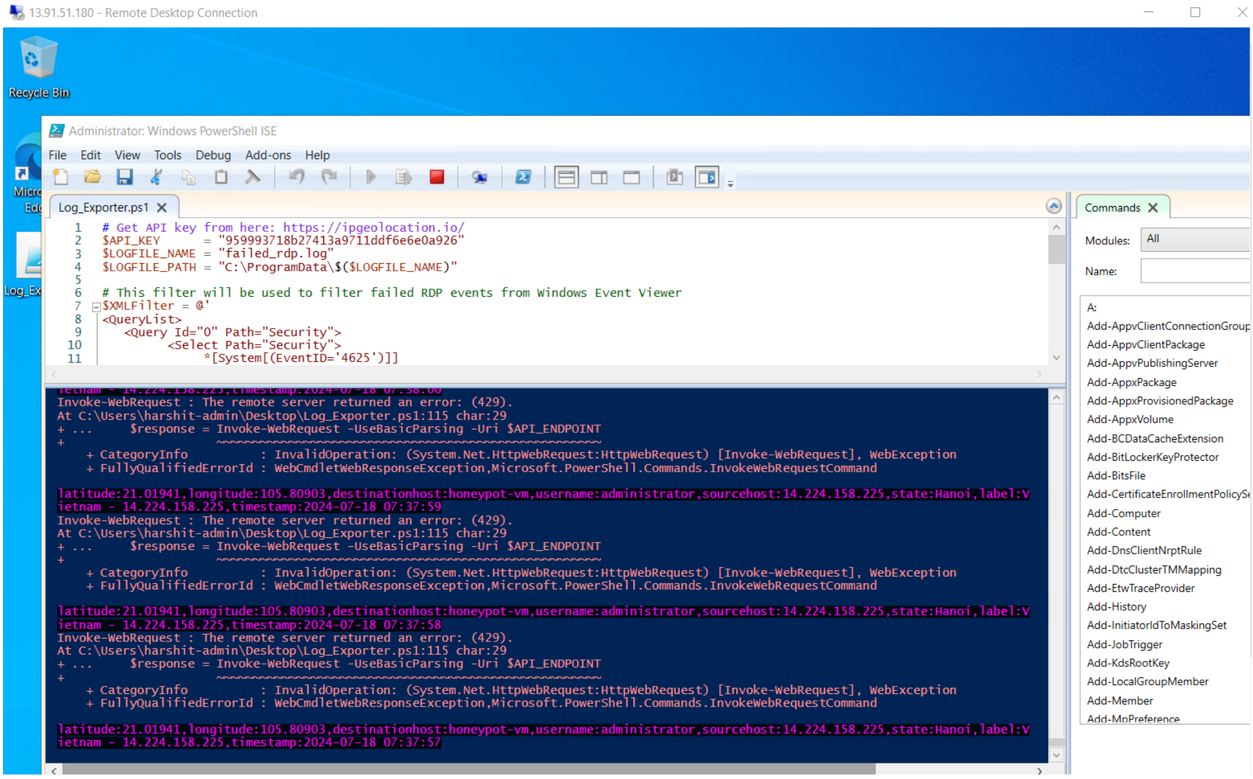
Once the environment is set up and the script is running, you will start seeing live RDP brute force attacks plotted on the Microsoft Sentinel map. This visualization helps understand the geographic distribution of attacks and identify patterns or hotspots of malicious activity.

Dataflow Diagram


Honeypot VM on Azure
Event Logs
Captured by the honeypot VM
PowerShell Script
Extracts IP addresses from event logs
Geolocation API
Converts IP addresses to geographic locations
Custom Logs
Created with geolocation data
Microsoft Sentinel
:
Ingests custom logs and visualizes them on a map

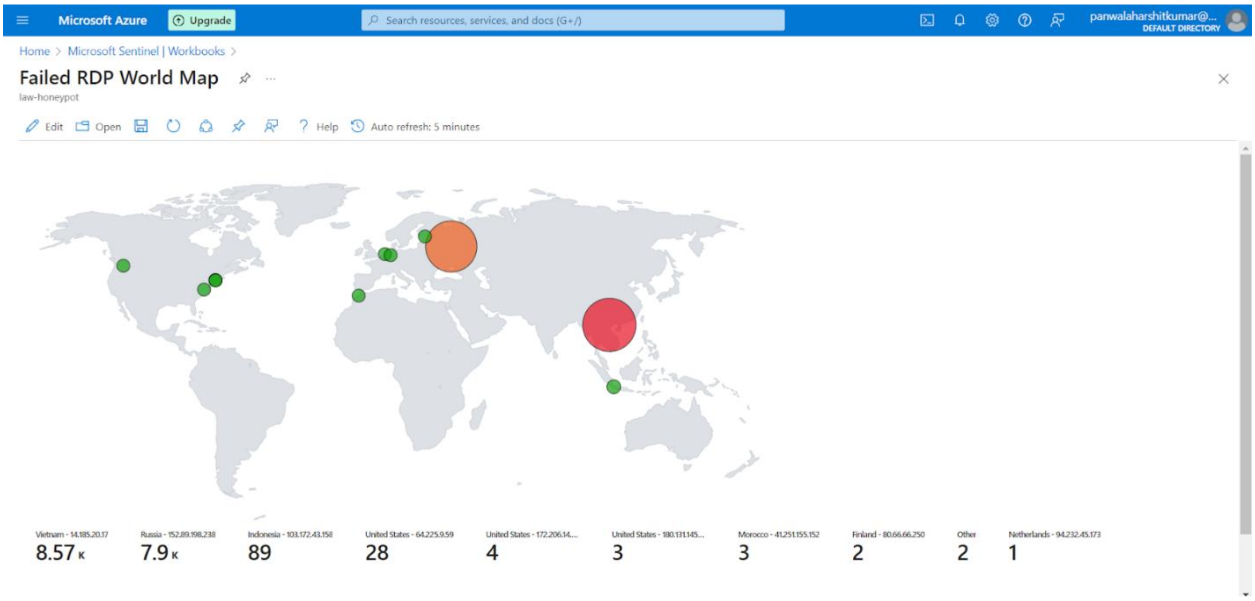
Final Output

- **World Map of Incoming Attacks After 24 Hours**: This visualization shows the geographic distribution of failed RDP attacks, providing valuable insights into the origin of these attacks.



```powershell
# Get API key from here: https://ipgeolocation.io/
$API_KEY      = "959993718b27413a9711ddf6e6e0a926"
$LOGFILE_NAME = "failed_rdp.log"
$LOGFILE_PATH = "C:\ProgramData\$($LOGFILE_NAME)"

# This filter will be used to filter failed RDP events from Windows Event Viewer
$XMLFilter = @'
<QueryList>
   <Query Id="0" Path="Security">
         <Select Path="Security">
              *[System[(EventID='4625')]]
```

```
ietnam - 14.224.158.225,timestamp:2024-07-18 07:38:00
Invoke-WebRequest : The remote server returned an error: (429).
At C:\Users\harshit-admin\Desktop\Log_Exporter.ps1:115 char:29
+ ...     $response = Invoke-WebRequest -UseBasicParsing -Uri $API_ENDPOINT
+                     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-WebRequest], WebException
    + FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand

latitude:21.01941,longitude:105.80903,destinationhost:honeypot-vm,username:administrator,sourcehost:14.224.158.225,state:Hanoi,label:V
ietnam - 14.224.158.225,timestamp:2024-07-18 07:37:59
Invoke-WebRequest : The remote server returned an error: (429).
At C:\Users\harshit-admin\Desktop\Log_Exporter.ps1:115 char:29
+ ...     $response = Invoke-WebRequest -UseBasicParsing -Uri $API_ENDPOINT
+                     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-WebRequest], WebException
    + FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand

latitude:21.01941,longitude:105.80903,destinationhost:honeypot-vm,username:administrator,sourcehost:14.224.158.225,state:Hanoi,label:V
ietnam - 14.224.158.225,timestamp:2024-07-18 07:37:58
Invoke-WebRequest : The remote server returned an error: (429).
At C:\Users\harshit-admin\Desktop\Log_Exporter.ps1:115 char:29
+ ...     $response = Invoke-WebRequest -UseBasicParsing -Uri $API_ENDPOINT
+                     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-WebRequest], WebException
    + FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand

latitude:21.01941,longitude:105.80903,destinationhost:honeypot-vm,username:administrator,sourcehost:14.224.158.225,state:Hanoi,label:V
ietnam - 14.224.158.225,timestamp:2024-07-18 07:37:57
```


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
panwalaharshitkumar@...
DEFAULT DIRECTORY
Home > Microsoft Sentinel | Workbooks >

Failed RDP World Map

law-honeypot

Vietnam - 14.185.20.17	Russia - 152.89.198.238	Indonesia - 103.172.43.158	United States - 64.225.9.59	United States - 172.206.14....	United States - 180.131.145...	Morocco - 41.251.155.152	Finland - 80.66.66.250	Other	Netherlands - 94.232.45.173
8.57 K	7.9 K	89	28	4	3	3	2	2	1

Security Considerations

- Ensure the honeypot VM is isolated and does not contain sensitive data.
- Regularly update the script and VM to mitigate vulnerabilities.
- Monitor the performance impact on the VM due to logging and script execution.

Conclusion and Future Work

This project demonstrates the effectiveness of Microsoft Sentinel in monitoring and analyzing security threats in real-time. By using a honeypot setup and a custom PowerShell script, valuable insights into the geographic distribution of RDP brute force attacks can be gained, aiding in better understanding and mitigating such threats.

Future Enhancements

- Automate the deployment and configuration of the honeypot VM and Microsoft Sentinel.
- Integrate additional data sources for a comprehensive security analysis.
- Implement alerting mechanisms for real-time threat response.