Future Ready Talent - Project Documentation

Name – Chirag Kadam

Project Title – (SIEM)Azure Sentinel Cloud Security Project With LIVE Graphical Representation

[ MAP ] Of Incoming Attacks Using Azure Sentinel.

**Project Statement**

This project aims to implement a robust Security Information and Event Management (SIEM) solution using Microsoft Azure Sentinel to enhance the security posture of our organization's cloud infrastructure. The project will not only ensure efficient data collection and analysis but will also provide real-time graphical representations of security events and incidents, enabling our security team to make informed decisions promptly. By leveraging Azure Sentinel's capabilities and live graphical representations, we will proactively monitor and respond to security threats, ultimately safeguarding our cloud assets and data from potential risks.

**Description -**

As we delve deeper into the realm of cybersecurity, it becomes crucial to understand the significance of creating a Virtual Honeypot and effectively analyzing failed login attack logs. In this project, we have taken the necessary steps to enhance our cybersecurity measures by implementing a comprehensive approach.

To begin with, we established a Virtual Machine (VM) designed as a honeypot, intentionally vulnerable to external attacks. By doing so, we created an environment that allows us to observe and analyze the tactics employed by potential adversaries.

To streamline the analysis process, we developed a Log Analytics Workbench capable of ingesting all the failed login logs from the VM. Leveraging the power of Microsoft Sentinel, we seamlessly integrated the logs into our system for further examination. This integration empowers us to gain valuable insights into the nature and scale of the attacks we encounter.

To facilitate the collection of pertinent information, we utilized a PowerShell script. This script effectively captures the IP addresses associated with each failed login attempt. By extracting this data from the VM's Event Viewer, specifically the Windows Log and Security section under Failed Audits, we acquire critical information regarding the origin of these attacks.

Taking our investigation a step further, we leveraged the capabilities of https://ipgeolocation.io/ to obtain geographic details for the identified IP addresses. With this information in hand, we generated a detailed file that provides a comprehensive overview of the geographical locations associated with the attacks. This file was then seamlessly integrated into our Azure Log Analytics Workspace, allowing for further analysis and exploration.

By harnessing the power of the logs and their associated geographic data, we are able to leverage Microsoft Sentinel to create a visually compelling graphical representation. This representation allows us to identify patterns and trends, enabling us to make informed decisions regarding our cybersecurity strategy. Through this process, we gain valuable insights into the origins of these attacks, empowering us to fortify our defenses accordingly.

In conclusion, by implementing a Virtual Honeypot and leveraging the capabilities of Microsoft Sentinel, we have fortified our cybersecurity infrastructure. The seamless integration of logs, IP geolocation data, and advanced analytics empowers us to detect attack patterns, identify vulnerabilities, and proactively enhance our security measures. By staying vigilant and leveraging these tools, we are better equipped to protect our systems and data from potential threats.

**Azure Services Used –**

Virtual Machine

Azure Defender For Cloud

Azure Log Analytics Workspace

Azure Sentinel

**Other Services Used –**

Windows Viewer

API – IP Geolocation

PowerShell Scripts

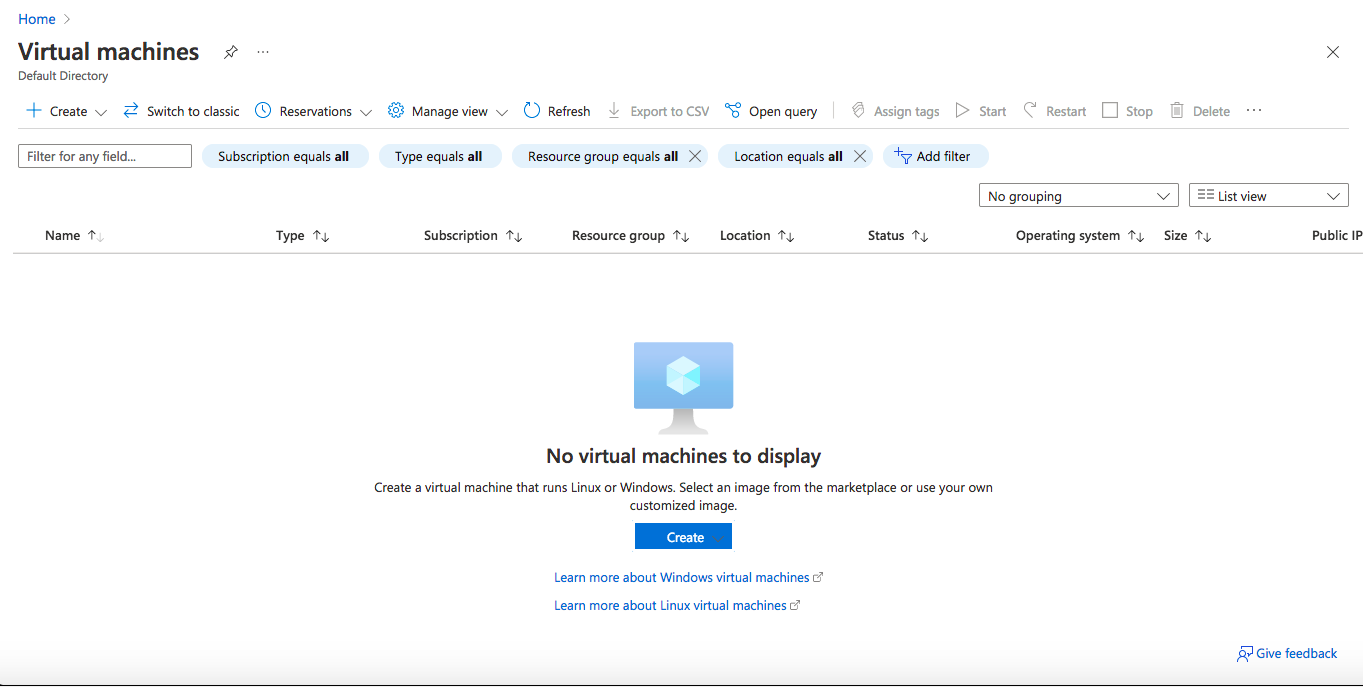
**Environment Used-**

VM – Windows 10

System – Windows 11

**Project Walkthrough**

* **Create an Azure free account, sign into my Azure Portal**
* **Click on virtual machine tab, create virtual machine :**



o Subscription- Azure For Students

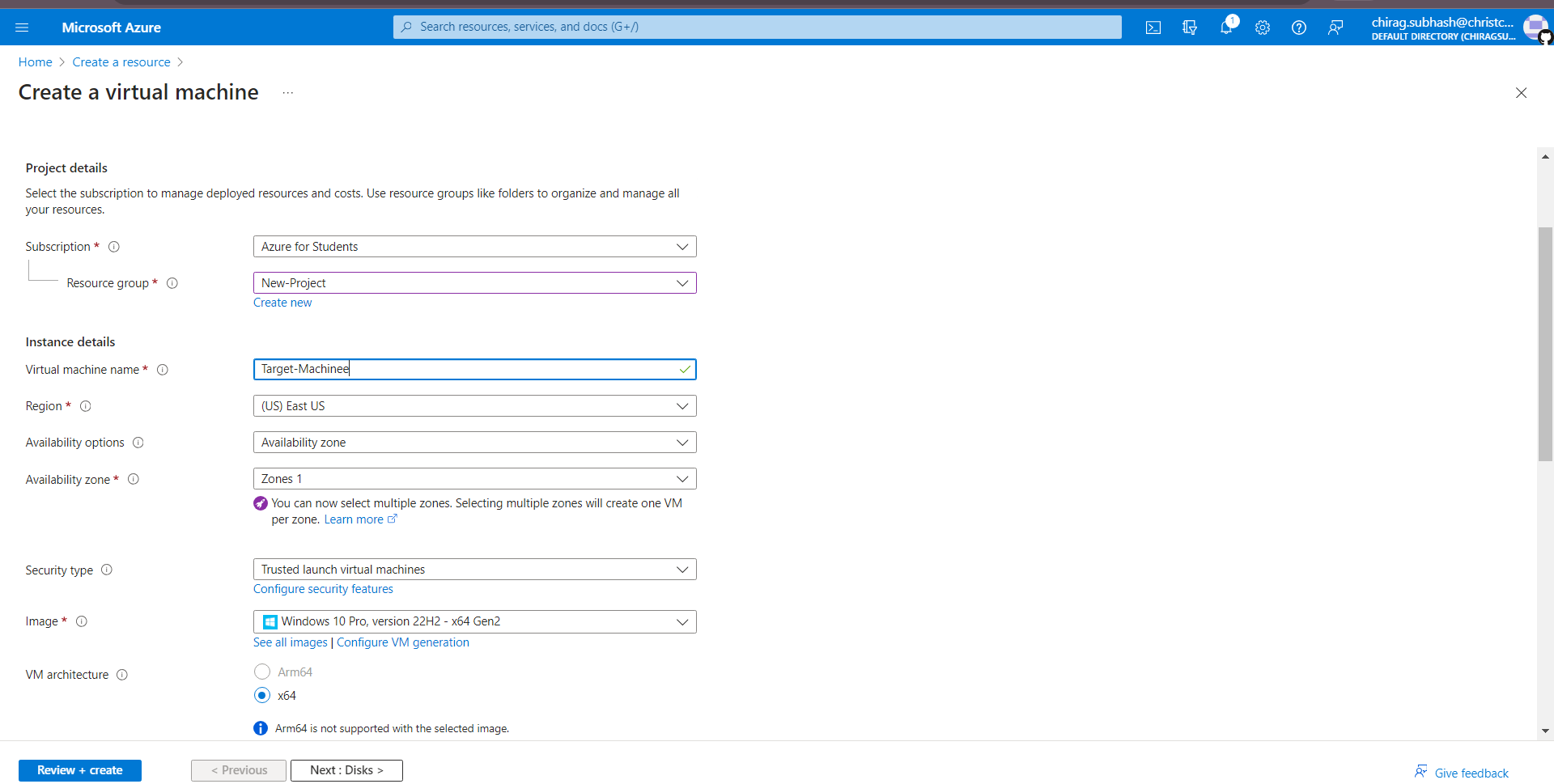
o Resource group- name New Project

o Virtual machine name- Taget-Machine

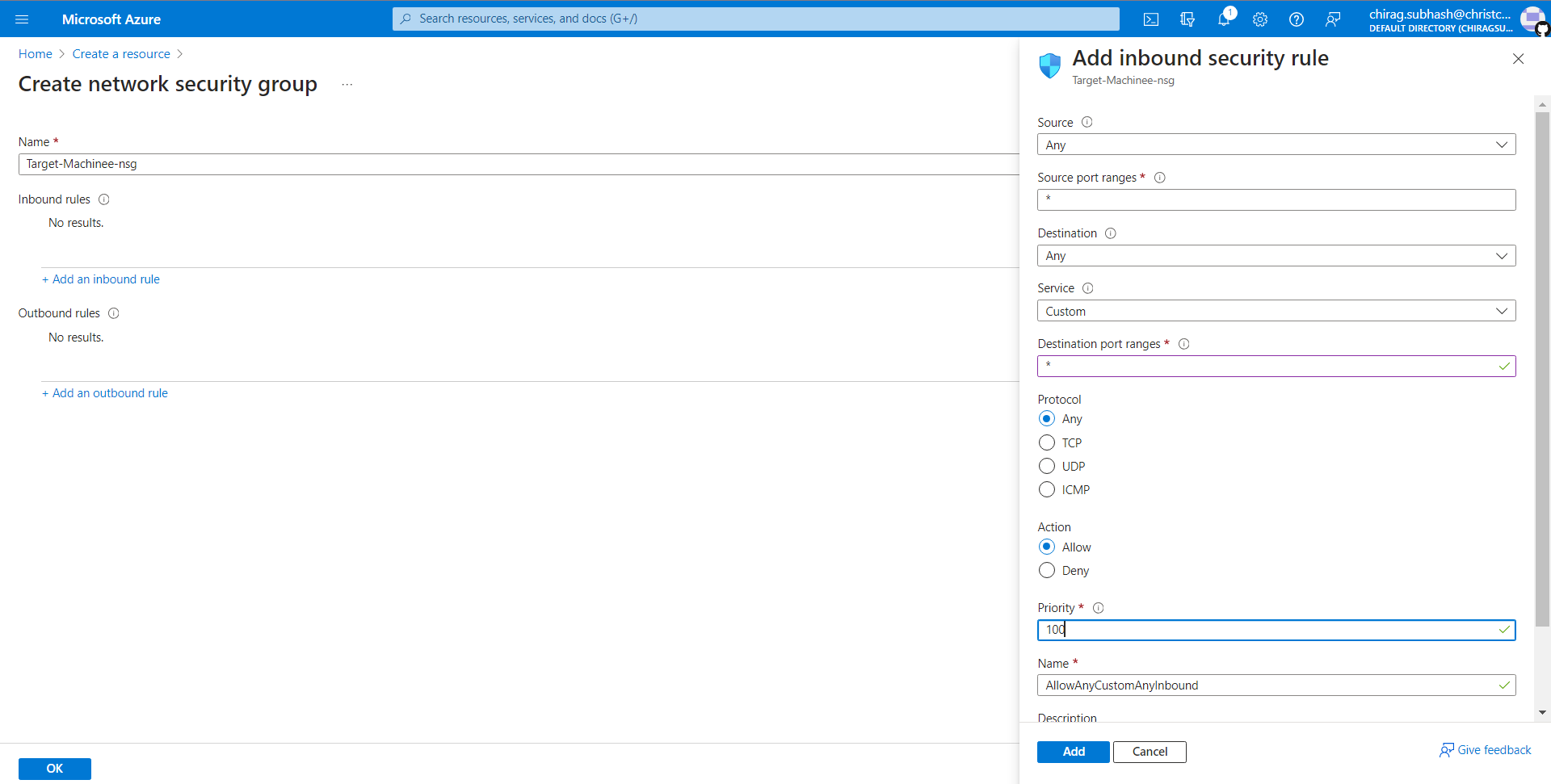
o Region- EAST US

o Leave rest of options on this page as default and created username and password for VM

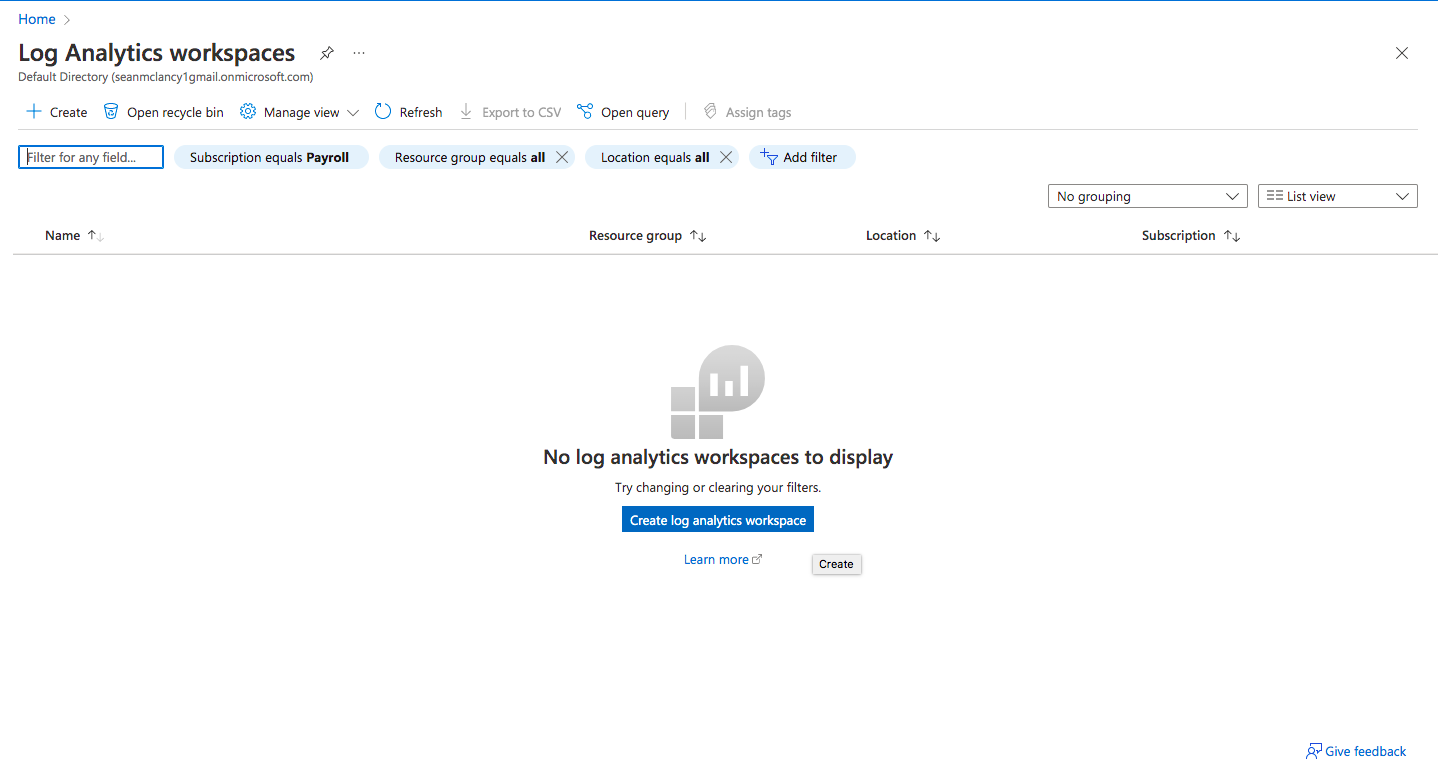
o Leave disks tab as default



* Click on Networking tab- Find NIC network security group- change to advanced
* Find configure network security group- Click “create new”
* Remove default inbound rule- add an inbound rule- Port ranges=\*, priority=100, name= DANGER\_UNSECURE o Click Review+Create



• Create Log Analytics workspace:

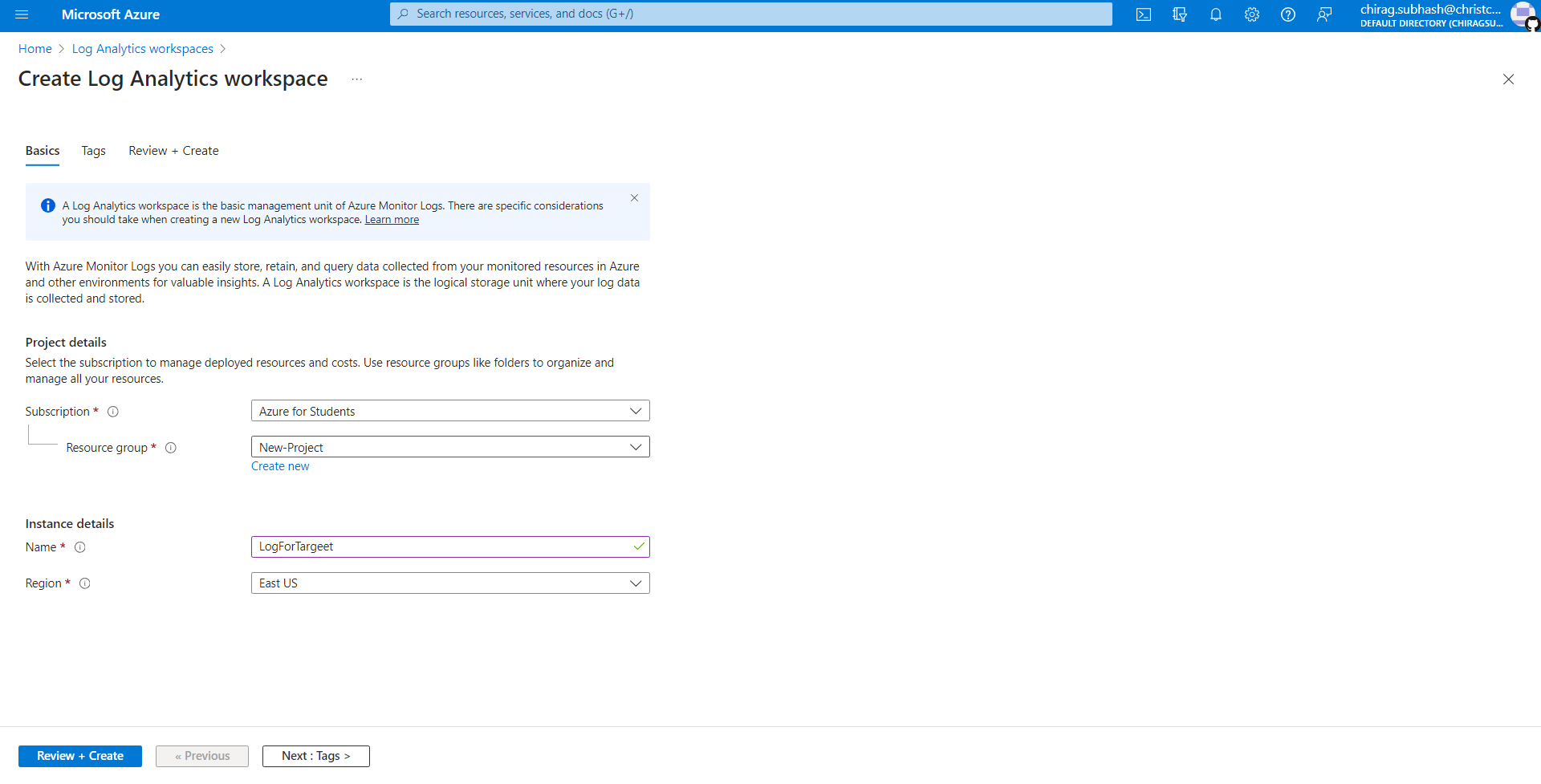


o Subscription- Pay as you go

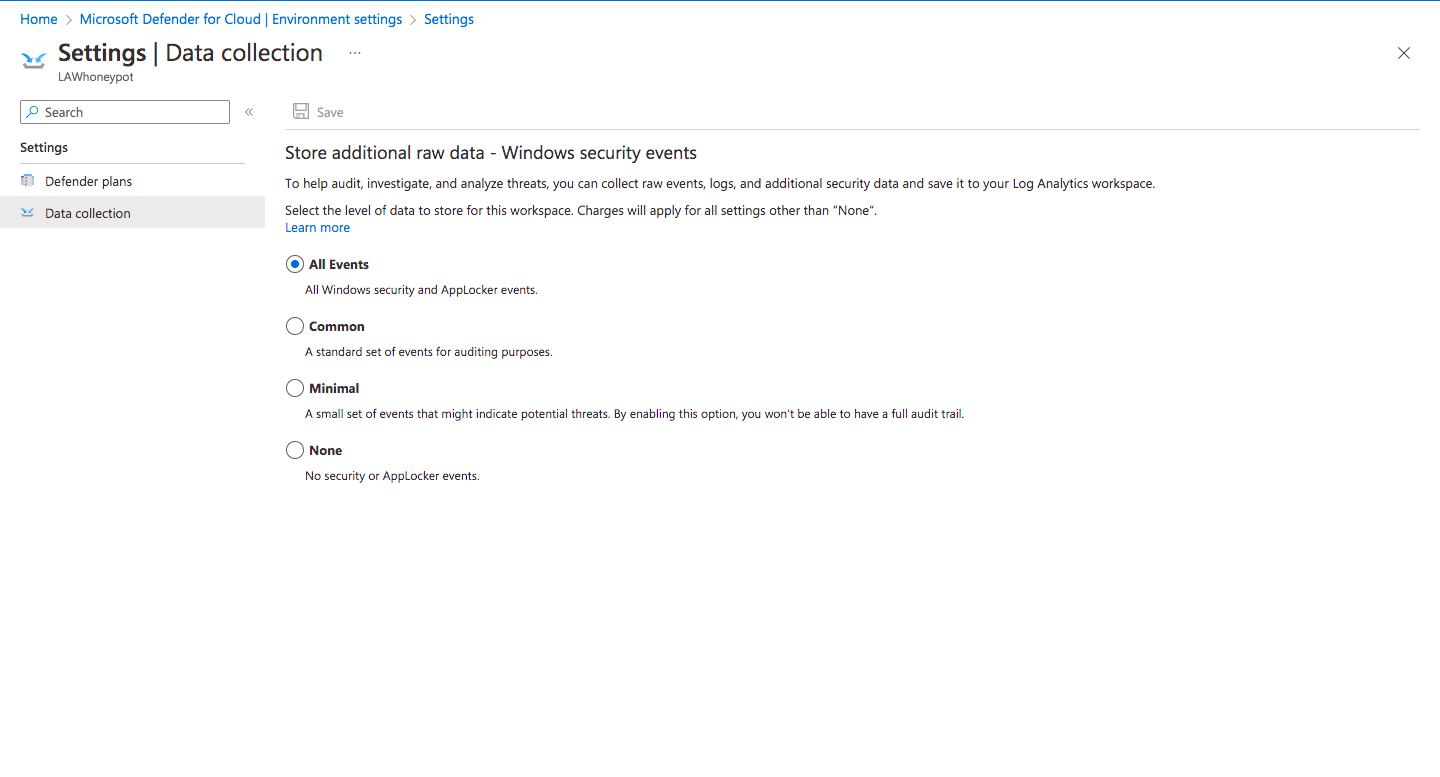
o Resource group- Choose New-Project

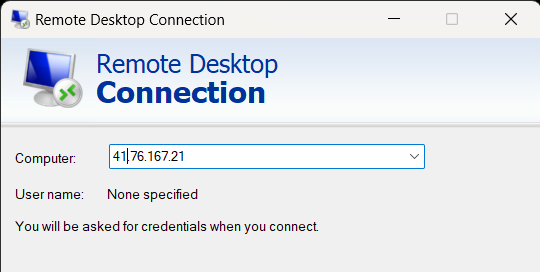
o Name- LogForTarget

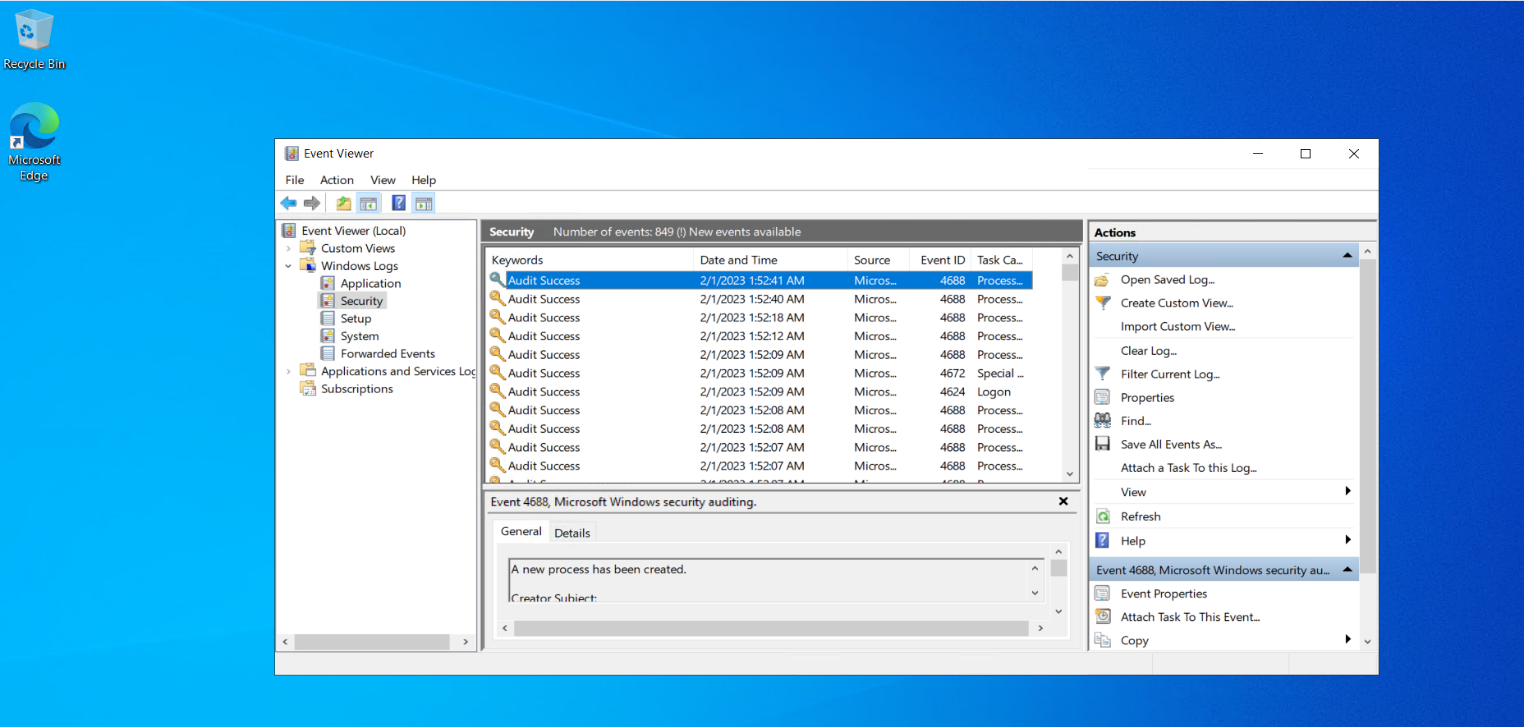
o Region- East US



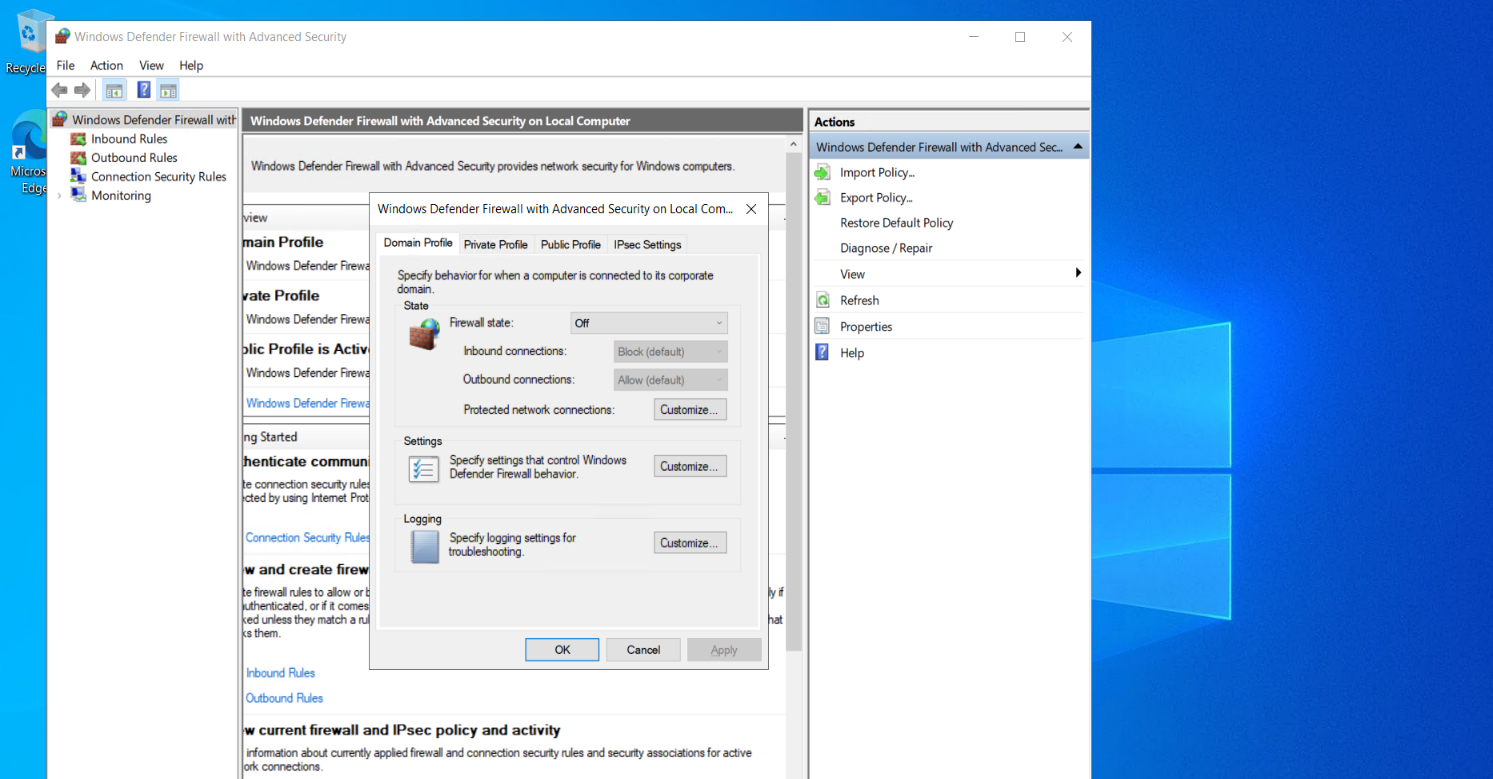
* Go to Microsoft Defender for the Cloud
* Find management section- go to Environment Settings- click LogForTarget :
* Go to “SQL servers on machines” and turn off the setting for it as we won’t be needing it.
* Click save o Click “Data collection”- Choose “All Events”- Save



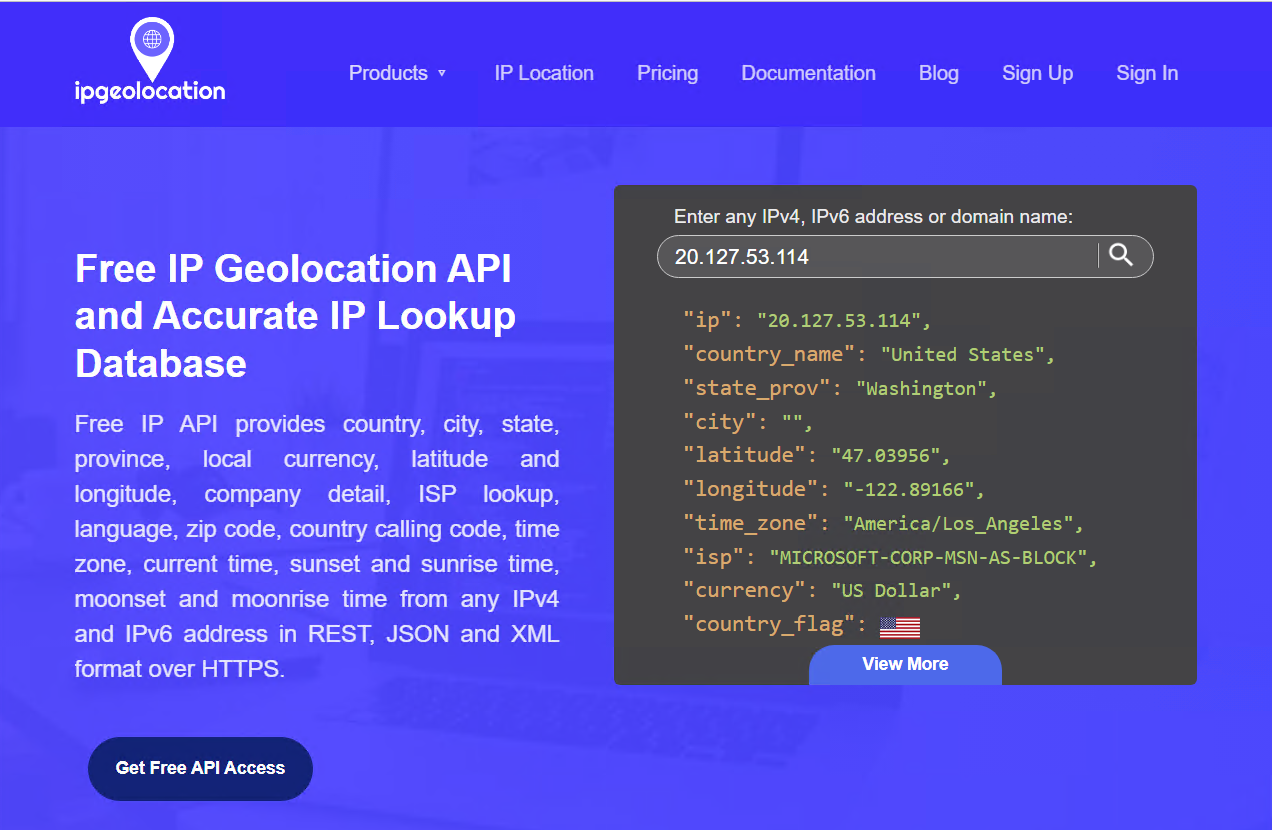
* Go back to Log Analytics Workspace
* Find virtual machine section- Click “Connect” to connect workspace to VM
* Setup Microsoft Sentinel- Find and click create
* Click Log Analytics workspace that was created- Add
* Find Virtual Machine- Go to Public IP Address and copy
* Open remote desktop on computer o paste the IP- Connect
* Go to more choices- Use a different account
* Use username and password that was used for the VM
* Log in
* 
* Now Operate within Virtual Machine
* Setup browser
* Click start- Find “Event Viewer”- Open



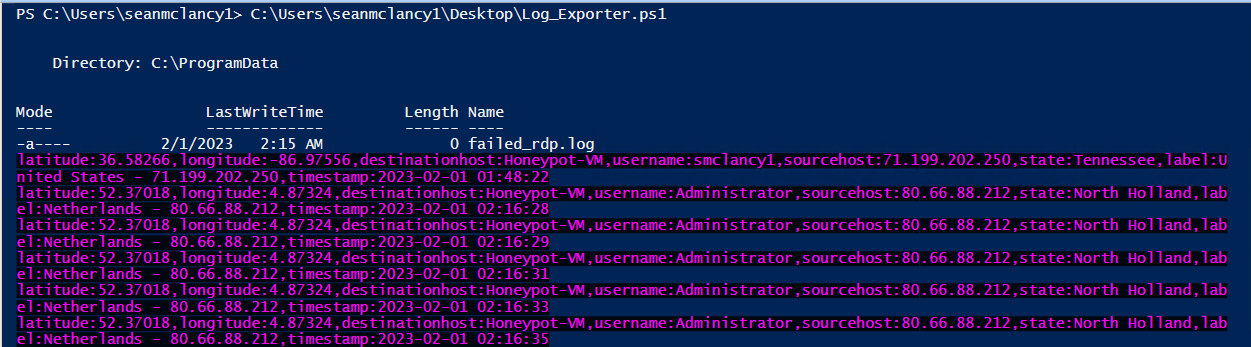
* Go to windows logs- Click security
* Find any event with keywords “Audit Failure” (This shows failed attempts to log into VM)- Find Source Network Address
* Click start- open windows defender firewall
* Click Windows Defender Firewall Properties
* Go to domain/private/public profile- Firewall state: Off
* Apply
* Close out everything



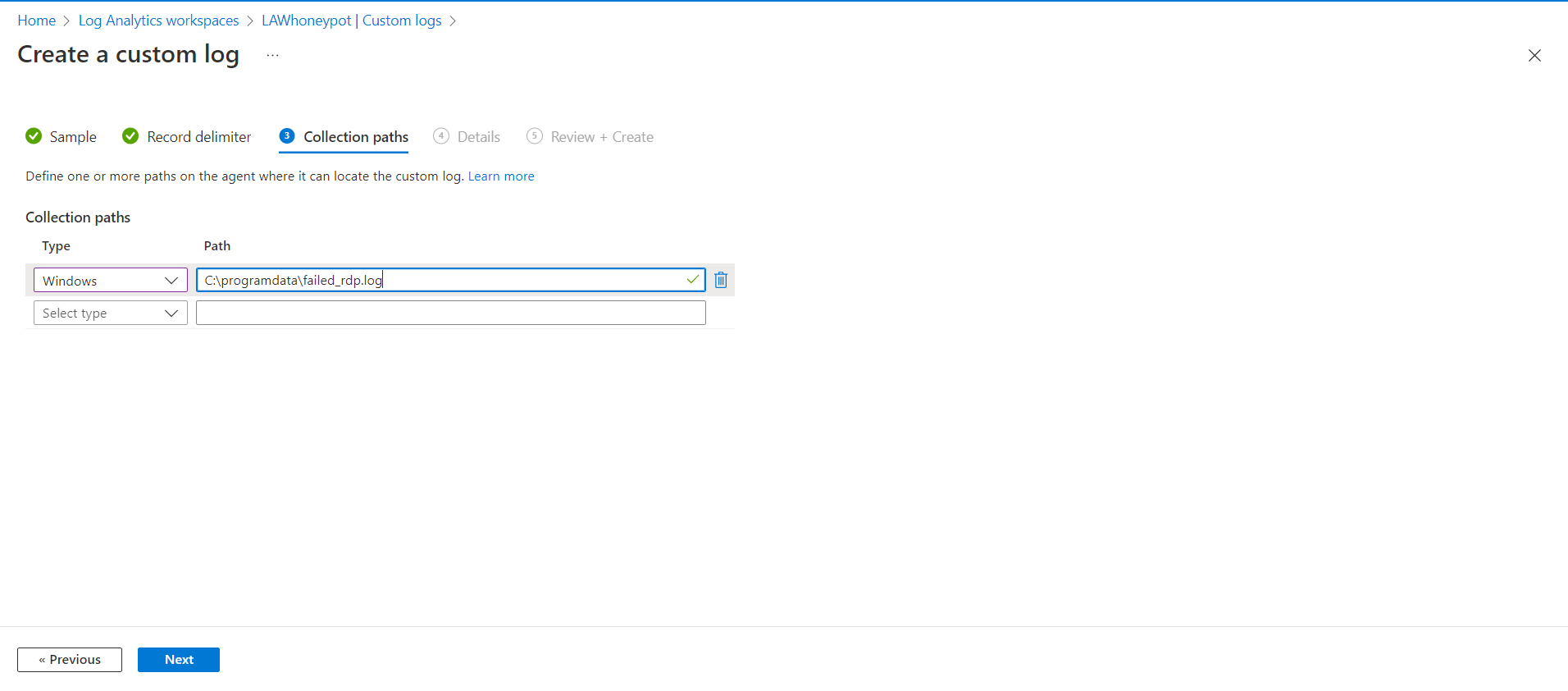
* Download PowerShell script- Custom\_Security\_Log\_Exporter.ps1
* Open Windows Powershell ISE
* Paste and save script as Log\_Exporter
* Go to https://ipgeolocation.io/
* Signup- Copy API Key
* Paste into Script
* Run Script



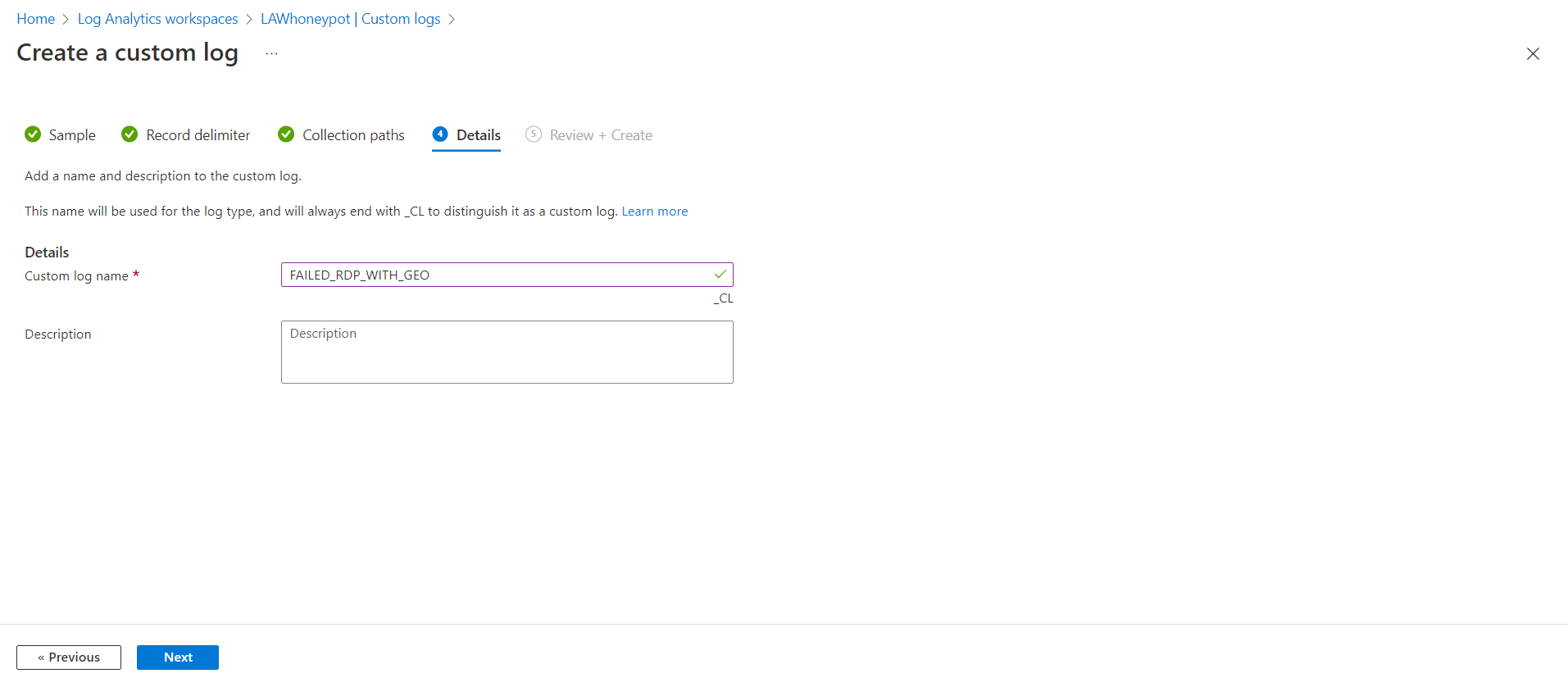
* The script is now running and will pull the failed attempts IP addresses, insert into the ipgeolocation website, takes that information and creates a failed login file.



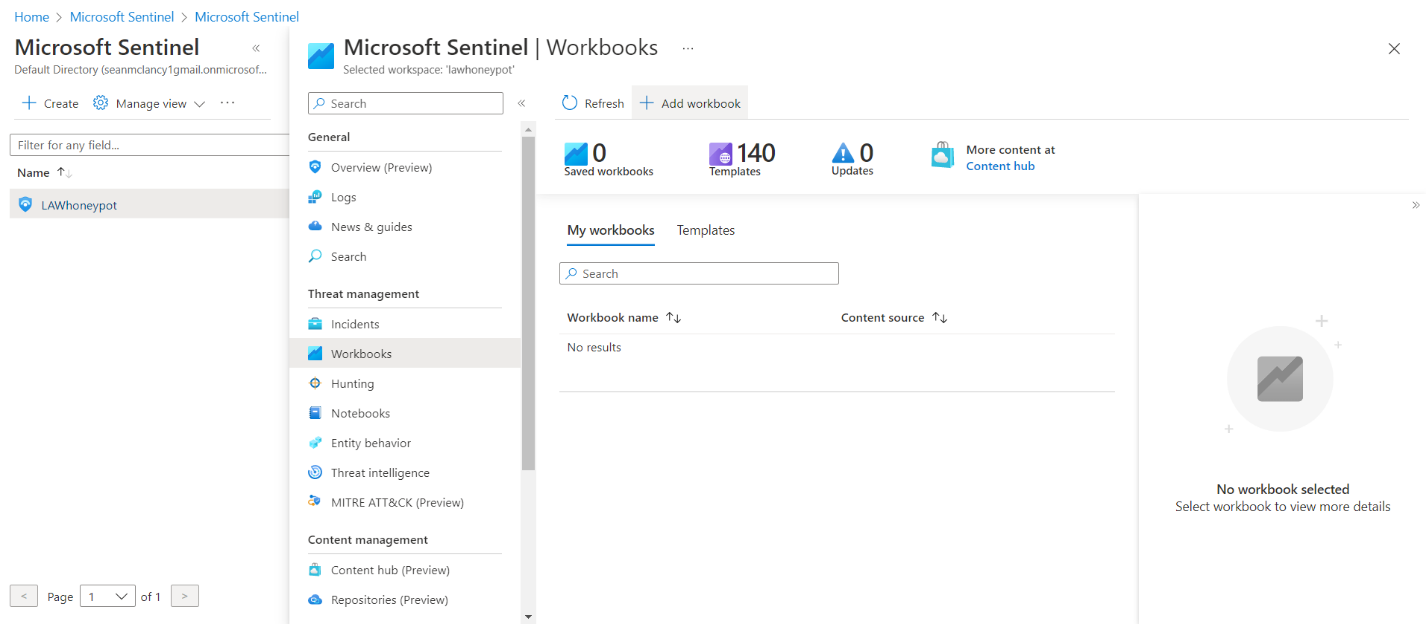
* Find failed\_rdp file
* Copy contents of file
* Go back to main computer
* Open notepad- Paste contents of file, Save on desktop as failed\_rdp
* Go to azure portal- Log analytics, click on workspace
* Go to custom log- add custom log o select file in custom log
* Click next, under Collection paths choose Windows for type
* For path- copy the path from the VM- C:\ProgramData\failed\_rdp.log \* Needs to be accurate



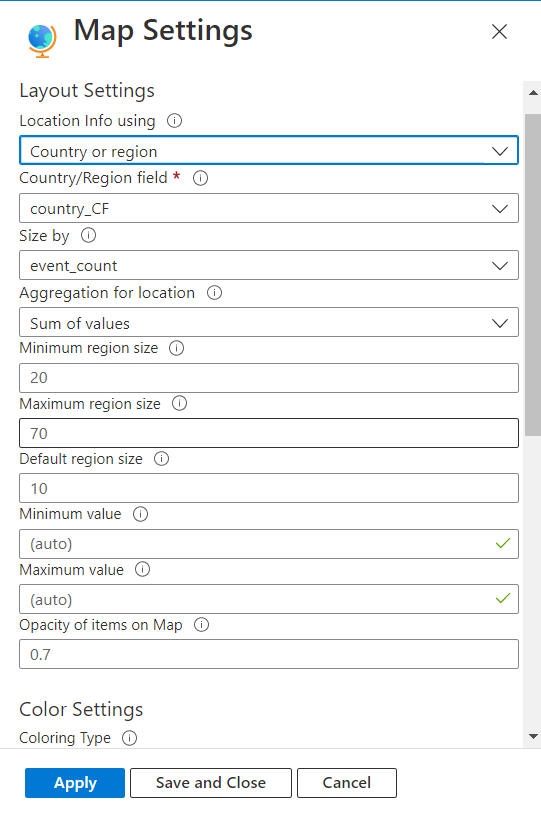
* Click next, Details Custom log name= FAILED\_RDP\_WITH\_GEO
* Next, and create



* Go to Logs o Type-> FAILED\_RDP\_WITH\_GEO\_CL
* Run (Will now show all failed logs)
* Click one of the logs- Extract fields o Highlight latitude- Change field title to latitude and Field type as Numeric, Extract o (If search results bring up other data than latitude then modify highlight)
* Repeat with longitude, destination host (text, not numeric), username, sourcehost, state, country, label, and timestamp
* Re-run script, Wait to repopulate with new fields
* Open new tab, go to azure portal
* Type Sentinel- click on log\_analytics\_workspace\_honeypot
* Click on “Workbooks”- Add new



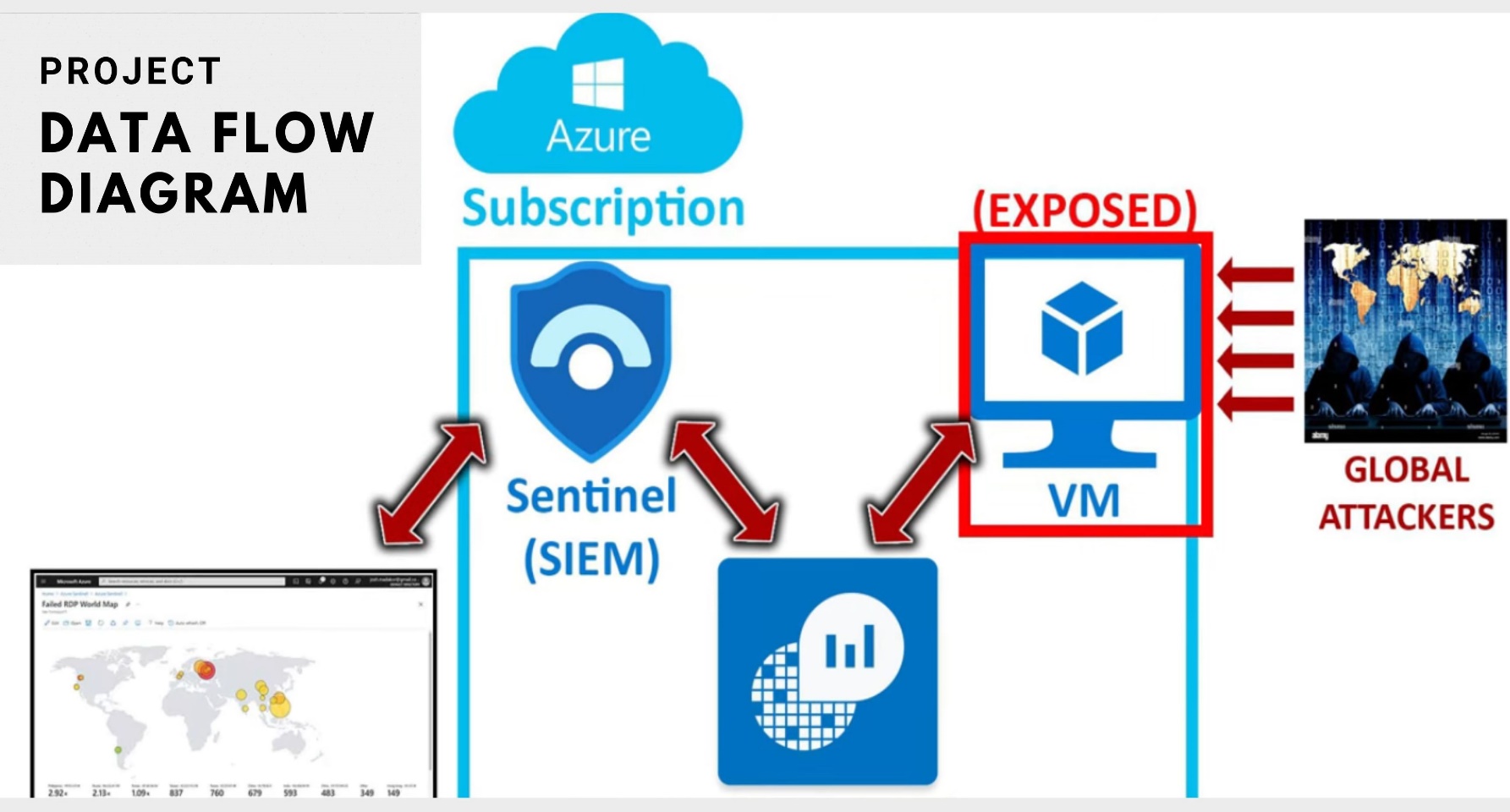
* Edit- remove default widgets o Add Query- type in-> FAILED\_RDP\_WITH\_GEO\_CL | summarize event\_count=count() by sourcehost\_CF, latitude\_CF, longitude\_CF, country\_CF, label\_CF, destinationhost\_CF | where destinationhost\_CF != “samplehost” | where sourcehost\_CF != “”
* Run Query o Fill in settings



Save with title: Failed RDP World Map, US Central for location

Click done editing, will now have map with the results of the attacks done on the HoneyPot [Target-Machine] VM.

**Project Data Flow Diagram**



**Conclusion**

**Project Conclusion-**

In this project, we have successfully implemented a comprehensive Security Information and Event Management (SIEM) solution using Microsoft Azure Sentinel. Our primary objective was to enhance cloud security by proactively identifying and mitigating incoming attacks in real-time. Throughout the project, we have leveraged Azure Sentinel's powerful features and integrated various data sources to create a unified security monitoring platform.

Achievements Our project has yielded several noteworthy achievements: Deployment of Azure Sentinel: We have successfully deployed Azure Sentinel, a cloud-native SIEM solution, which enables real-time security monitoring and threat detection in Azure and hybrid environments. Data Source Integration: We have integrated multiple data sources into Azure Sentinel, including Azure Activity Logs, Office 365 audit logs, Azure Security Center alerts, and custom logs, allowing us to have comprehensive visibility into our cloud environment. Incident Detection and Alerting: We have configured advanced detection rules and playbooks to identify security incidents. When a potential threat is detected, automated alerts are triggered, providing the security team with real-time notifications. Custom Dashboards and Reporting: We have created custom dashboards and reports in Azure Sentinel to visualize security data. These graphical representations help security analysts quickly assess the security posture and respond to incidents effectively. Live Attack Map: One of the most significant achievements is the implementation of a Live Attack Map, which provides a dynamic, graphical representation of incoming attacks in real-time. This map helps visualize the geographic distribution of attacks, attack types, and their severity, enabling security teams to respond promptly to emerging threats.