Live Cyber Attack Cloud VM Honeypot with Azure Project

Abstract

This project investigates real-time cyberattacks targeting a Cloud Virtual Machine (VM) hosted on Microsoft Azure. The project utilizes a honeypot, a decoy system mimicking a vulnerable Windows 10 machine, to attract and observe live cyberattacks, specifically focusing on Remote Desktop Protocol (RDP) brute-force attempts.

Methodology:

1. **Honeypot Deployment:** A Windows 10 VM is deployed within the Azure cloud environment, configured to resemble a real system while remaining isolated from the production network.
2. **Attacker Geolocation:** A PowerShell script is developed to parse attack logs and extract attacker IP addresses. Geolocation data for these IPs is then obtained to understand the geographical distribution of attack sources.
3. **Log Collection and Analysis:** The script further automates the process of collecting logs from the honeypot VM and forwarding them to Azure Log Analytics, a centralized log management service. This facilitates comprehensive analysis of attack patterns and trends.
4. **Attack Observation:** The honeypot remains accessible to the public internet, allowing attackers to launch RDP brute-force attempts. Azure Sentinel, a Security Information and Event Management (SIEM) solution, is integrated to collect and analyze attack data in real-time.

Expected Outcomes:

- Gaining insights into the volume and origin of global RDP brute-force attacks.
- Evaluating the effectiveness of Azure Sentinel in real-time attack detection and visualization.
- Demonstrating the value of honeypots for proactive security monitoring and threat intelligence gathering.
- Highlighting the ongoing need for robust cybersecurity measures to protect cloud-based resources.

Overall, This project contributes to a deeper understanding of real-world cyberattacks, SIEM capabilities, and the importance of proactive security practices in the cloud environment.

Project Content

Introduction

The digital landscape is a constant battleground, with malicious actors perpetually devising new methods to breach systems and steal data. In this ever-evolving threat environment, organizations require robust security strategies to stay ahead of cyberattacks. This project delves into the fascinating world of live cyberattacks, specifically focusing on Remote Desktop Protocol (RDP) brute-force attempts, by leveraging a honeypot within the Microsoft Azure cloud platform.

Honeypots: This project utilizes a honeypot, a meticulously crafted decoy system designed to mimic a vulnerable Windows 10 machine. By deploying this honeypot within the Azure cloud environment, I create a tempting target for attackers, allowing me to observe their tactics and techniques in real-time. This approach offers a unique perspective on actual attack patterns, providing valuable insights that traditional security measures might miss.

Azure Sentinel: To effectively monitor and analyze attack activity on the honeypot, I integrate Azure Sentinel, a powerful Security Information and Event Management (SIEM) solution offered by Microsoft Azure. Azure Sentinel acts as our central hub, collecting and analyzing data from the honeypot in real-time. This enables me to detect and visualize RDP brute-force attempts as they occur, providing a clear understanding of the attack landscape.

Beyond Detection: This project goes beyond simply observing attacks. I leverage a custom-developed PowerShell script to extract attacker IP addresses from the honeypot logs. Utilizing geolocation services, I then uncover the geographical distribution of attacks, revealing the global reach of RDP brute-force campaigns. Additionally, the script automates the process of collecting logs from the honeypot and forwarding them to Azure Log Analytics, a centralized log management service within Azure. This comprehensive log analysis allows us to identify attack patterns and trends, providing valuable insights into attacker behavior.

Why This Project Matters

By investigating real-world cyberattacks, this project aims to achieve several key objectives:

- **Empowering Security Teams:** Gaining a deeper understanding of the volume and origin of global RDP brute-force attacks allows security teams to prioritize their efforts and implement more effective defense strategies.
- **Evaluating Azure Sentinel:** The project assesses the effectiveness of Azure Sentinel in real-time attack detection and visualization, showcasing its value as a security tool for Azure environments.
- **Advancing Proactive Security:** By demonstrating the power of honeypots for threat intelligence gathering, the project emphasizes the importance of proactive security measures in protecting cloud-based resources.

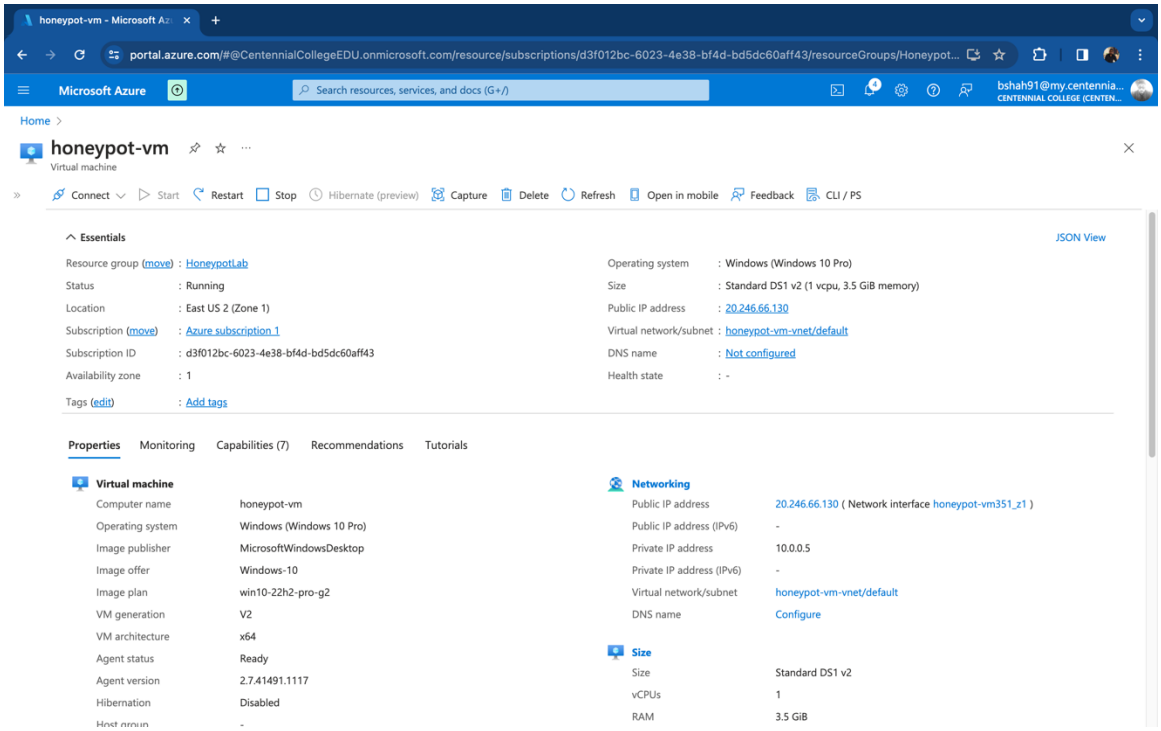
Methodology

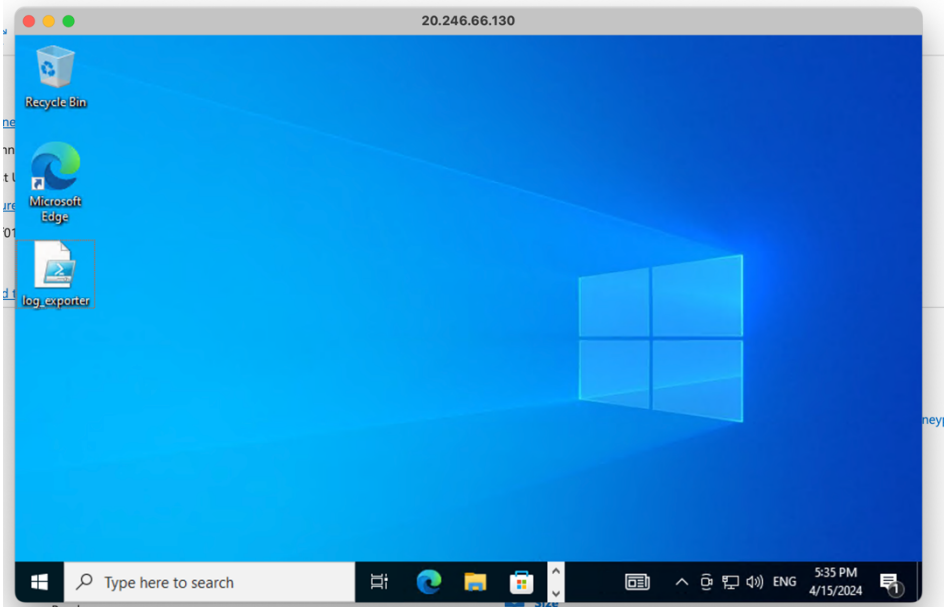
1. Honeypot Deployment

The first step is to create a MS Azure virtual OS Windows 10.

1.1 Creating Virtual Machine

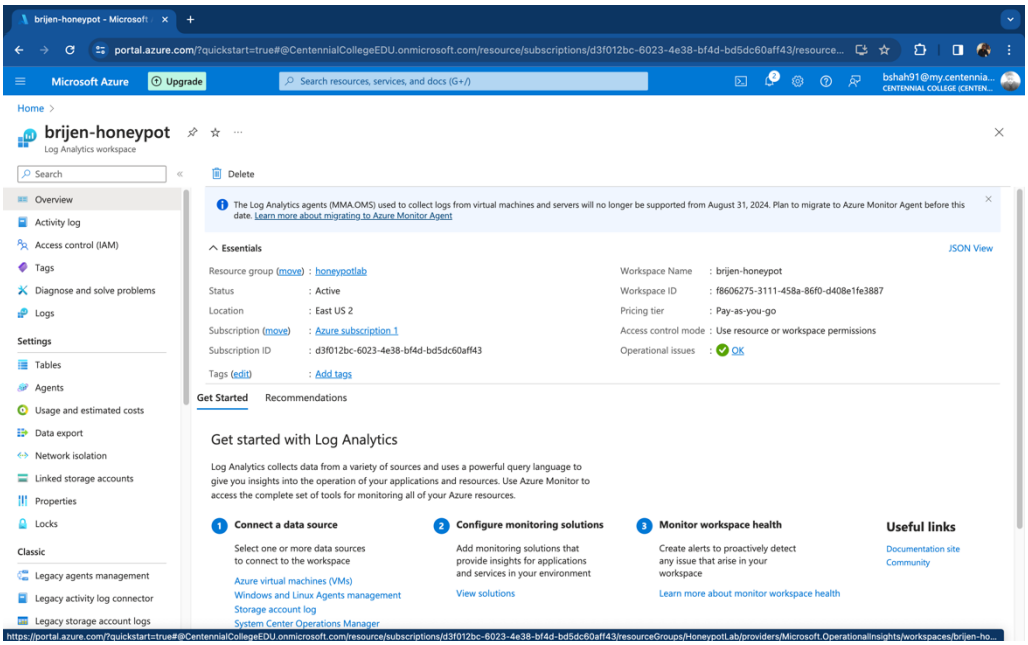
I have created Windows 10 VM in Azure allowing all traffic and made virtual machine discoverable. After creating virtual machine, I have successfully logged in RDP for further configuration.





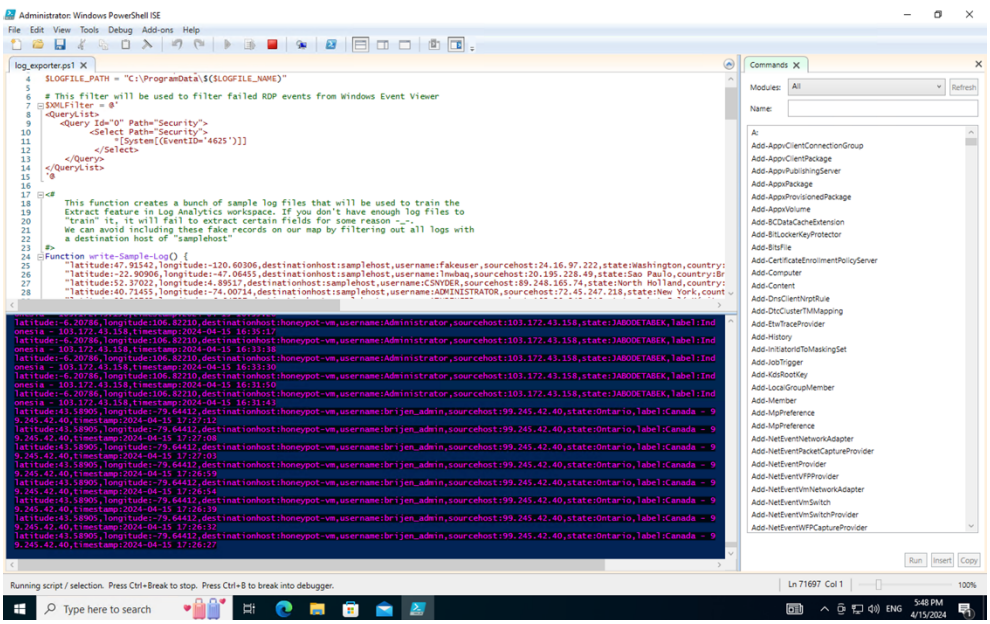
1.2 Azure Log Analytics

I have created Log Analytics workspace in Azure for log analysis and connected VM to the log Analytics workspace.



1.3 PowerShell script to gather failed RDP logs

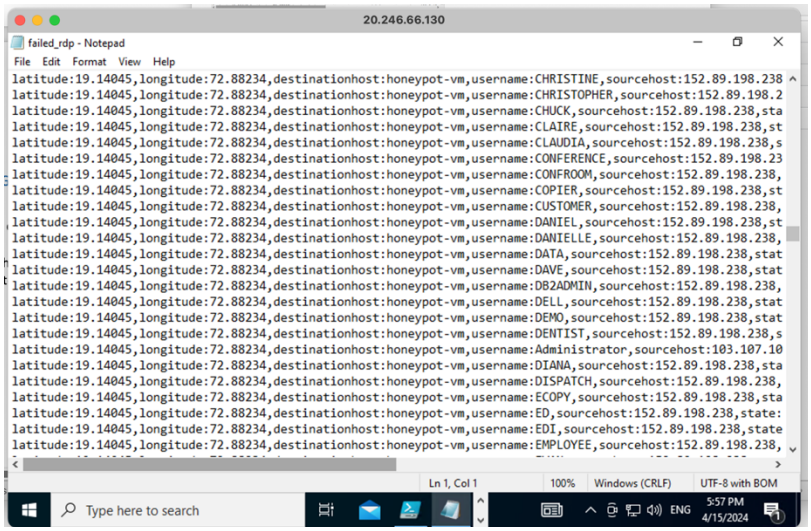
I have used PowerShell script to gather and save logs of failed RDP attack data into VM. The log file named as “failed_rdp.txt”.



2. Attacker Geolocation

2.1 Use of Geolocation.io API

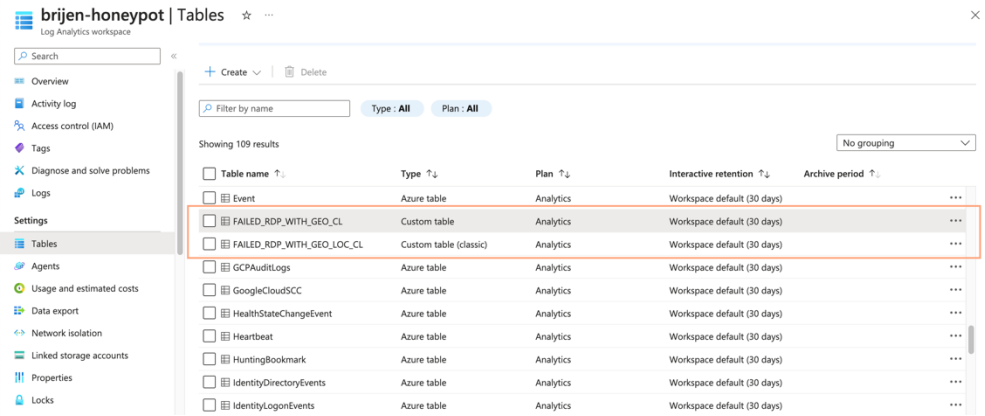
To gather geolocation of Attacker IP, I am using Geolocation.io API. This API is used in Shell Script to convert latitude and longitude of the attacker Ip and store it into log file.



3. Log Collection and Analysis

3.1 Custom Log Creation

Firstly, I have created custom log in Log Analytics workspace. The selection I have made for custom log ins MMA based in which I have submitted sample log to train log analysis. After creation of custom log, I have integrated the collection path of VM log in the custom log, by which the data is accessible to fetch in custom log.

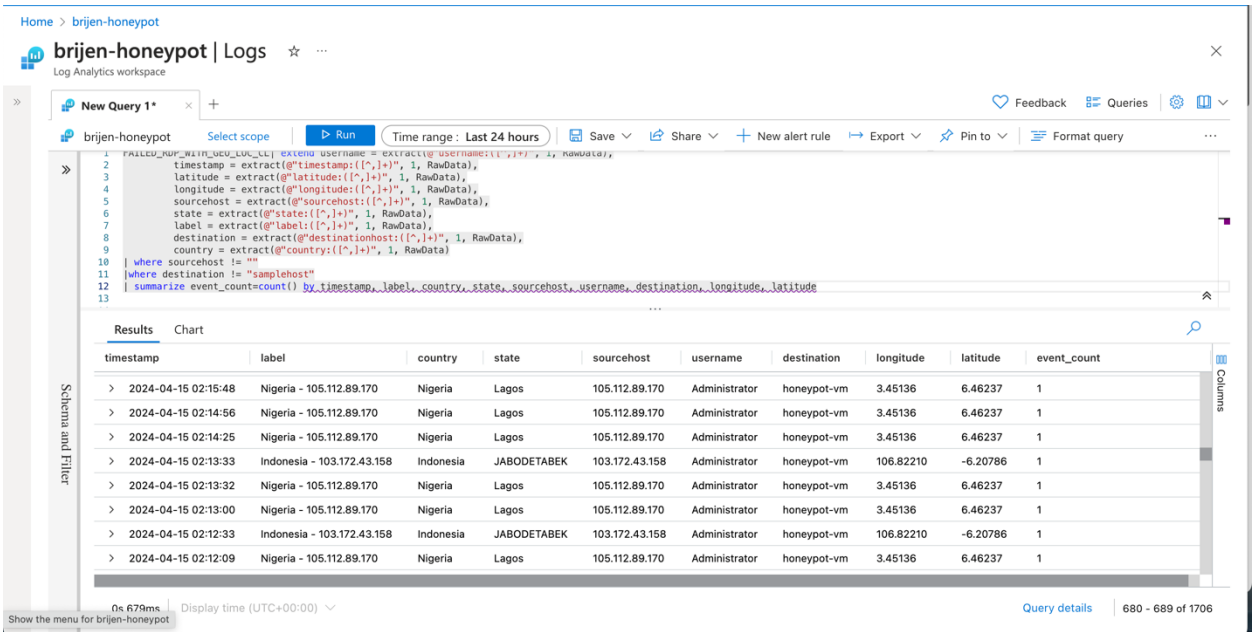


3.2 Query Custom Log for Analysis

To get data from custom log, I have created query that can generate the accessible data with data extract columns such as latitude, longitude, hostname, country and so on. Querying log helps to identify proper functioning of the system and bifurcate the log data which can be used for further analysis.

The below Query I generated helps in data extraction with fields and log analysis:

```
" 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 sourcehost != ""
|where destination != "samplehost"
|summarize event_count=count() by timestamp, label, country, state, sourcehost, username,
destination, longitude, latitude"
```

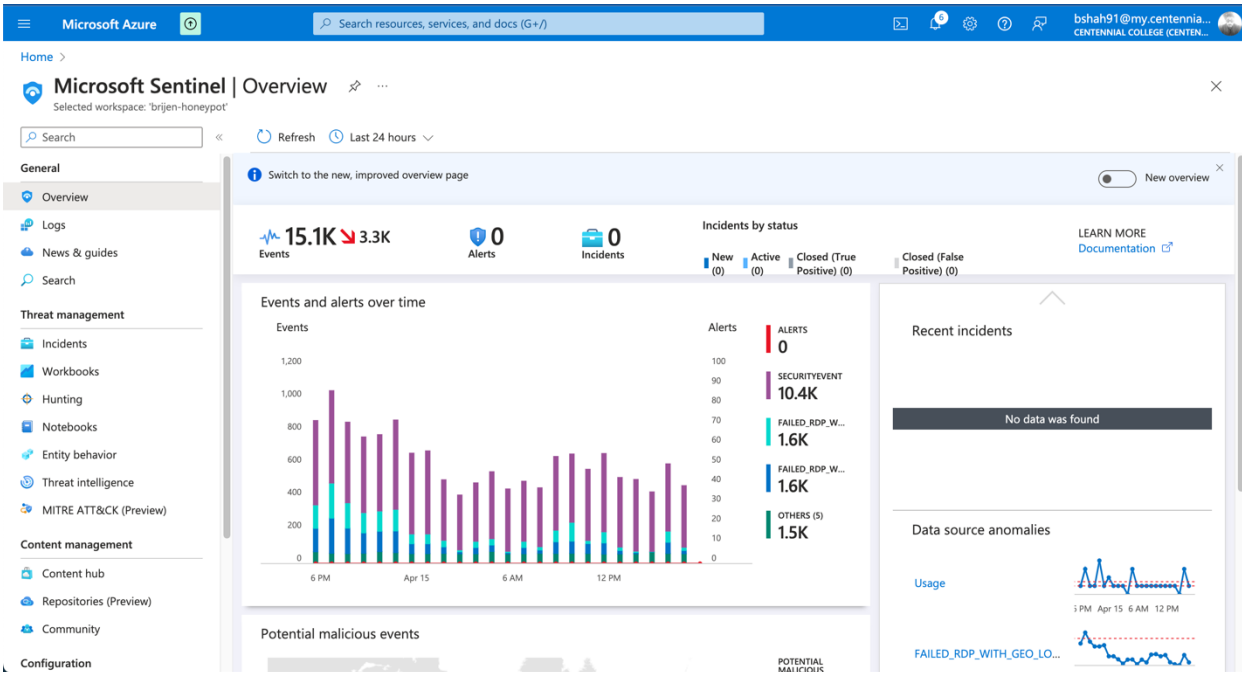


4. Attack Observation

Azure Sentinel (SIEM) tool provides excellent data and log visualization which I have utilized to display the ongoing live attacks.

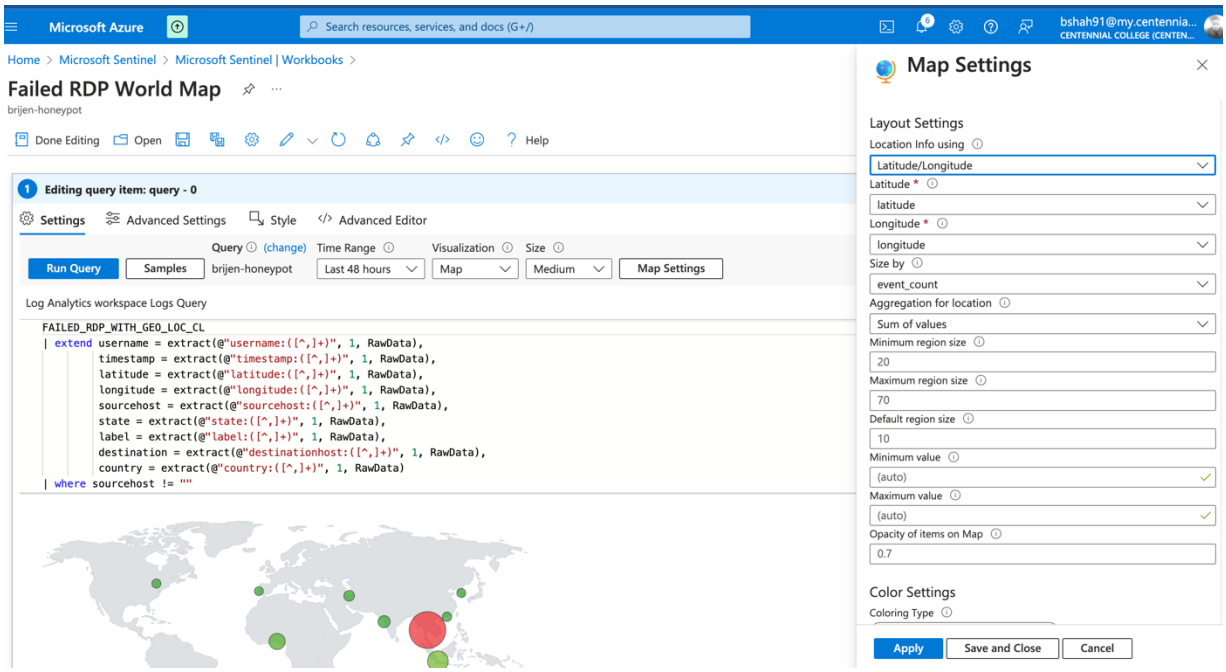
4.1 Azure Sentinel setup

Azure Sentinel offers outstanding data visualization for analyzing data, alerts, and potential threats. I've linked the Log Analytics workspace with Sentinel to enhance access to logs and data. The following image displays the cumulative failed Remote Desktop Protocol (RDP) connection attempts on the honeypot virtual machine.

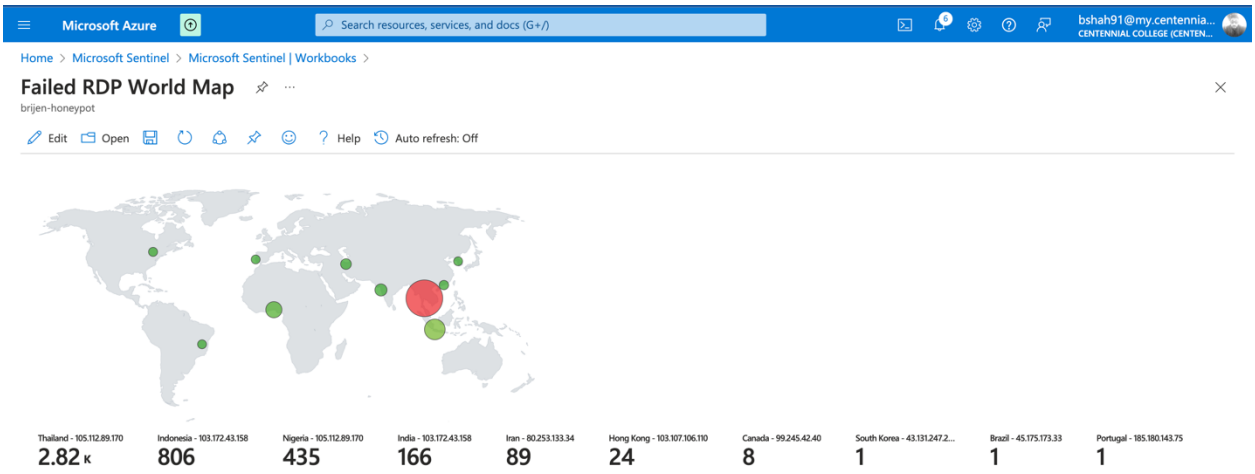


4.2 Azure Sentinel Map Visualization

To create a Map visual in the Sentinel SIEM tool, I've initiated a new workbook. I cleared out all default visuals and established a fresh one by specifying a query parameter. This parameter is based on the query I've employed before for Log Analysis. I've configured the visual to display as a map and set the time range for 48 hours. To ensure the map is accurate, I've utilized latitude and longitude for geolocation and adjusted the size based on event count to represent total occurrences.



The live attacks on cloud VM starts taking place when system becomes discoverable to the internet. The below image shows the ongoing live cyber-attacks specially RDP brute force on the system. The dashboard provides a visual representation of attacks with the geographical origin of the attacks.



Conclusion

This project successfully investigated real-world cyberattacks targeting a Cloud Virtual Machine (VM) deployed within Microsoft Azure. Utilizing a honeypot configured as a vulnerable Windows 10 system, the project attracted and observed live attacks, specifically focusing on Remote Desktop Protocol (RDP) brute-force attempts. The integration of Azure Sentinel, a SIEM solution, facilitated real-time attack detection and visualization.

The project confirmed the effectiveness of honeypots in attracting and observing live cyberattacks. The image from the Azure Sentinel workspace provided a compelling visual representation of the attack landscape, with red dots on the world map indicating numerous RDP brute-force attempts originating from various geographical locations. This highlights the global scale and prevalence of such attacks.

The project also demonstrated the value of Azure Sentinel in real-time attack detection and monitoring. By analyzing the data collected by Azure Sentinel, we gained valuable insights into attack patterns and origins. This knowledge is crucial for security teams to prioritize their efforts and implement effective defense strategies.

Overall, this project underscores the importance of proactive security measures to protect cloud-based resources. By deploying honeypots and leveraging SIEM tools like Azure Sentinel, organizations can gain valuable threat intelligence and improve their overall security posture. The project serves as a testament to the ever-evolving threat landscape and the need for continuous vigilance in the face of cyberattacks.