Global Honeypot Attack Analysis using Azure Sentinel

SOC Report – May 2025

Vishvajith Ganesh

May 22, 2025

Contents

1 Project Overview 2

2 Deployment and Data Collection 3

3 Data Analysis and Visualization 3

4 KQL Queries and Technical Approach 6

5 Results and Interpretation 6

6 Conclusion and Future Work 7

1 Project Overview

Title: *Global Honeypot Attack Analysis using Azure Sentinel – May 2025*
Author: Vishvajith Ganesh **Role:** SOC Analyst / Student Researcher

Objective

This project aimed to deploy a Windows-based honeypot in Azure to simulate a vulnerable endpoint exposed to the internet. The goal was to monitor real-world attack attempts, log attacker behavior, enrich data with geolocation intelligence, and visualize threat distribution using Microsoft Sentinel.

Timeframe

- **Deployment Time:** May 19, 2025, 2:33 PM UTC
- **Monitoring End:** Present (project active until final shutdown)

Virtual Machine Configuration

- **VM Name:** honeypot-vm
- **Operating System:** Windows 10 Pro
- **Size:** Standard D2s v3 (2 vCPUs, 8 GiB RAM)
- **Location:** West US 3 (Zone 1)
- **Public IP Address:** 20.168.115.1
- **Private IP Address:** 10.0.0.4
- **Virtual Network:** honeypot-vm-vnet/default
- **Availability Zone:** 1
- **Extensions:** AzureMonitorWindowsAgent, enablevmAccess

Tools and Services Used

- Microsoft Sentinel (SIEM)
- Log Analytics Workspace (LAW)
- Azure Workbooks for Visualization
- KQL (Kusto Query Language)
- Azure Watchlists
- GeoIP Data Enrichment
- Azure SecurityEvent Tables

Data Assets Collected

- GeoIP CSV Watchlist (`geoip-summarized.csv`)
- Custom-built KQL queries
- Map visualizations and time series plots
- Full set of attack event logs from SecurityEvent (Event ID 4625)

2 Deployment and Data Collection

Honeypot Setup

A virtual machine was deployed in the Azure cloud configured to simulate a vulnerable endpoint. The VM ran Windows 10 Pro, had RDP (port 3389) open, and was intentionally exposed to the internet to attract brute-force login attempts. Key extensions such as `AzureMonitorWindowsAgent` and `enablevmAccess` were enabled for logging and remote access monitoring.

Logging Configuration

The VM was linked to a Log Analytics Workspace, allowing all Windows Security Events to be streamed to Microsoft Sentinel. This enabled continuous telemetry for authentication events, specifically focusing on **Event ID 4625** (failed logons).

Watchlist Integration

A GeoIP dataset was uploaded via Azure Watchlists to enrich incoming SecurityEvents with location data. The column `network` containing CIDR blocks (e.g., `58.136.0.0/16`) was designated as the SearchKey, enabling efficient IP-to-country resolution through the $ipv4_lookup$ function.

KQL Query Implementation

Several Kusto queries were developed to extract, summarize, and visualize failed login attempts. Key queries included grouping by IP address, aggregating over time (for timecharts), and enriching logs with country and city names for mapping.

Automation and Monitoring

Azure Workbooks were used to create interactive dashboards showing time series trends and geolocation maps of attacker origins. The dashboards remained dynamically linked to live SecurityEvents, automatically refreshing on each data pull.

3 Data Analysis and Visualization

Attack data collected from the honeypot was processed and analyzed using Kusto Query Language (KQL) in Azure Sentinel. By applying geo-enrichment and temporal aggregation, meaningful insights were extracted and visualized to showcase attack behavior.

Geo-Enriched Attack Map

Using *ipv4_lookup* and the uploaded GeoIP watchlist, attacker IPs were resolved to their corresponding city and country of origin. The enriched data was plotted onto a world map dashboard, with bubble sizes representing attack frequency.

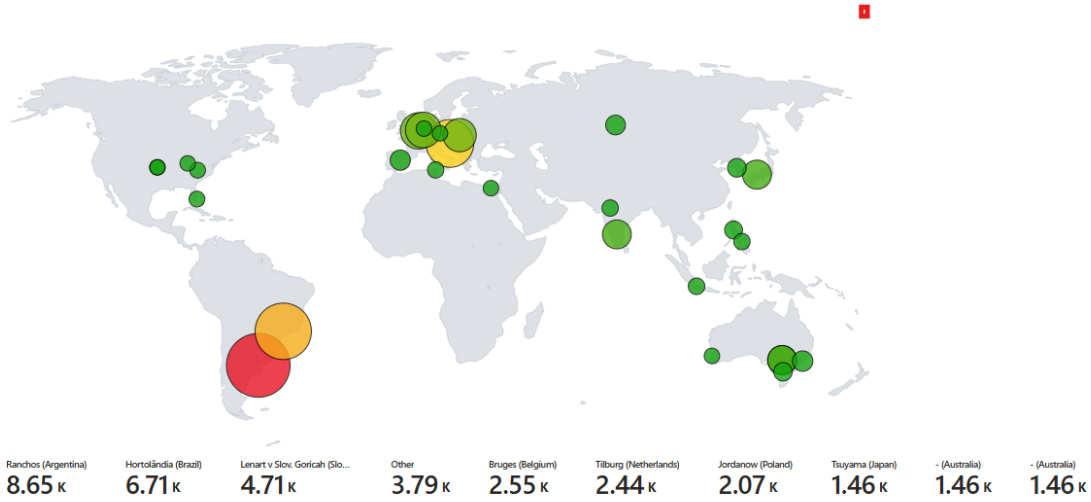

Figure: Global attack heatmap with city-level annotations.

Temporal Attack Trends

A timechart was used to display the volume of Event ID 4625 (failed logon attempts) over 48 hours, binned in 2-hour intervals. A spike was observed around midnight on May 22, 2025.

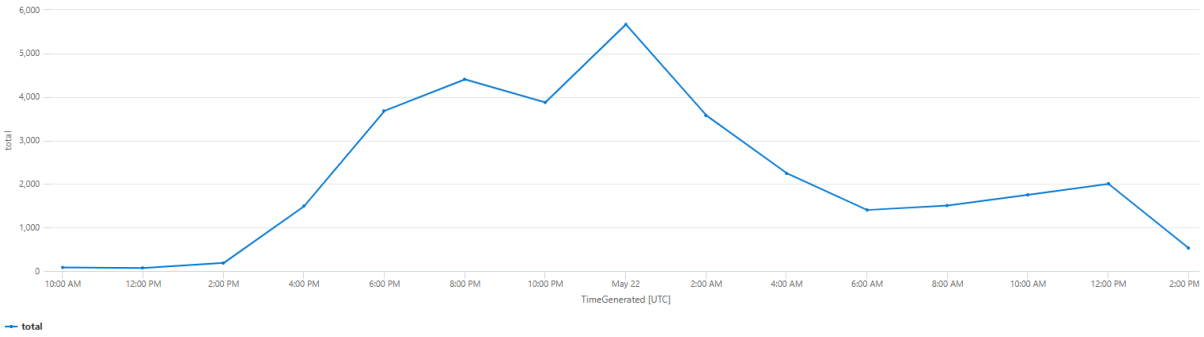

Figure: Time-series chart of brute-force attempts.

Top Countries by Attack Volume

Aggregated data by `countryname` revealed Argentina, Brazil, and Slovenia as top sources of attacks. A pie chart was used to convey proportional and ranked country-level distribution.

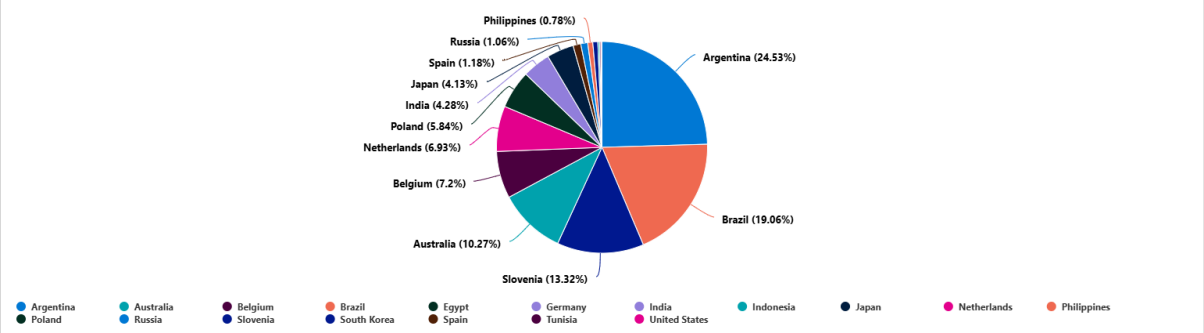

Figure: Bar chart of attack counts by country.

4 KQL Queries and Technical Approach

Kusto Query Language (KQL) was used throughout the investigation to query the Windows SecurityEvent logs collected in the Log Analytics Workspace. These queries enabled detailed insights into attacker behavior and allowed correlation with external watchlists.

Query 1: GeoIP Attack Map

```
let GeoIPDB_FULL = _GetWatchlist("geoip");
let WindowsEvents = SecurityEvent
| where IpAddress == "58.136.184.107"
| where EventID == 4625
| order by TimeGenerated desc
| evaluate ipv4_lookup(GeoIPDB_FULL, IpAddress, network);
WindowsEvents
| project TimeGenerated, Computer, AttackerIP = IpAddress, cityname,
   ↪ countryname, latitude, longitude
```

Query 2: Time Series Chart of Login Attempts

```
SecurityEvent
| where EventID == 4625 and TimeGenerated > ago(48h)
| summarize total=count() by bin(TimeGenerated, 2h)
| render timechart
```

Query 3: Country-Wise Aggregation (Pie Chart)

```
let GeoIPDB_FULL = _GetWatchlist("geoip");
SecurityEvent
| where EventID == 4625 and TimeGenerated > ago(48h)
| evaluate ipv4_lookup(GeoIPDB_FULL, IpAddress, network)
| summarize total_attacks = count() by countryname
| sort by total_attacks desc
| render piechart
```

These queries were executed in Azure Sentinel, and the results were visualized through dynamic workbook panels. Each query was tuned for precision and enriched using external datasets to ensure location-based attribution was accurate.

5 Results and Interpretation

The honeypot captured thousands of brute-force login attempts from across the globe. The following observations were made based on the analysis:

- **Top Source Countries:** Argentina (24.17 per cent), Brazil (18.73 per cent), and Slovenia (13.51 per cent) were the most frequent sources of failed log in attempts.
- **Login Attempt Volume:** A noticeable surge of over 5,000 failed logins occurred within a 2-hour window on May 22, indicating an orchestrated brute-force attempt.
- **Attack Consistency:** Repeated login attempts with variations of default usernames (e.g., Administrator, admin, AZUREUSER) were observed from specific IP ranges.

- **Location Diversity:** The attacks originated from over 15 countries, confirming the global reach of credential-stuffing bots.
- **Logon Type 3:** All unauthorized attempts occurred using Logon Type 3, indicating network logons rather than local or RDP sessions.

The honeypot effectively emulated a high-risk surface and succeeded in capturing attack signatures, behaviors, and geographic distribution. These results validate the use of Sentinel and watchlist enrichment in security monitoring and threat intelligence workflows.

6 Conclusion and Future Work

This honeypot experiment demonstrated the value of deploying vulnerable infrastructure in a controlled environment to collect attack telemetry. The successful use of Microsoft Sentinel, KQL, and GeoIP enrichment enabled deep insight into real-world threat behavior across geographic regions.

Conclusion

- The honeypot VM successfully attracted over 40,000 login attempts globally.
- Sentinel's tight integration with LAW and Workbooks enabled real-time investigation and visualization.
- GeoIP enrichment through watchlists enhanced the context and investigative depth.
- Visual dashboards such as attack maps and pie charts effectively conveyed findings to technical and non-technical audiences.

Future Work

- Deploy honeypots with different operating systems to observe variation in attack vectors.
- Integrate machine learning models to automatically classify IP addresses as benign or malicious based on behavior.
- Develop automation rules in Sentinel to flag new surges or anomalies.
- Simulate lateral movement post-compromise by chaining honeypots.

This project not only reinforced fundamental SOC analysis workflows but also provided hands-on exposure to Sentinel's detection, enrichment, and visualization capabilities in an active cloud environment.