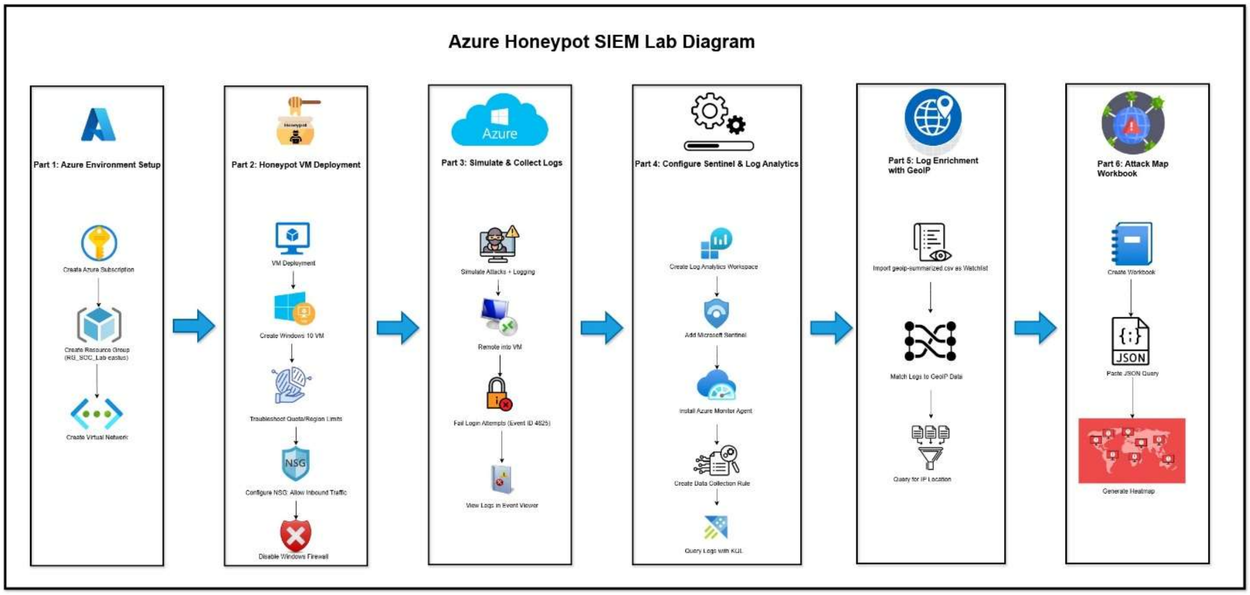
Azure Honeypot SIEM Threat Visibility Lab

Security Analyst & Cloud Engineer: Joseph Hardy
Date Completed: April 2025
Document Type: Threat Detection Lab Report & SIEM Implementation

Executive Summary

This lab report outlines the creation and deployment of a honeypot virtual machine in Microsoft Azure, integrated with Microsoft Sentinel for real-time threat monitoring. The objective was to simulate attacker behavior, forward event logs to a centralized SIEM, enrich data with geolocation details, and visualize threat sources using workbook heatmaps. The lab provided a hands-on opportunity to explore cloud logging pipelines, KQL analytics, and foundational SIEM operations in a real-world simulation.


Azure Honeypot SIEM Lab Diagram
Part 1: Azure Environment Setup
Create Azure Subscription
Create Resource Group (RG_SOC_Lab-eastus)
Create Virtual Network
Part 2: Honeypot VM Deployment
Honeypot
VM Deployment
Create Windows 10 VM
Troubleshoot Quota/Region Limits
NSG
Configure NSG: Allow Inbound Traffic
Disable Windows Firewall
Azure
Part 3: Simulate & Collect Logs
Simulate Attacks + Logging
Remote into VM
Fail Login Attempts (Event ID 4625)
View Logs in Event Viewer
Part 4: Configure Sentinel & Log Analytics
Create Log Analytics Workspace
Add Microsoft Sentinel
Install Azure Monitor Agent
Create Data Collection Rule
Query Logs with KQL
Part 5: Log Enrichment with GeoIP
Import geoip-summarized.csv as Watchlist
Match Logs to GeoIP Data
Query for IP Location
Part 6: Attack Map Workbook
Create Workbook
JSON
Paste JSON Query
Generate Heatmap

Project Objectives

- Deploy a Windows 10 honeypot VM in Azure
- Simulate malicious login attempts and monitor logs
- Forward logs to Microsoft Sentinel using Log Analytics
- Enrich log data using a GeoIP database

- Visualize attack origin data on a heatmap
- Practice Kusto Query Language (KQL) for threat analysis

Scope

In-Scope:

- Azure VM deployment & firewall configuration
- Security event monitoring (Event ID 4625)
- Sentinel log integration with Azure Monitor Agent
- GeoIP enrichment using watchlists
- KQL-based analysis and visualization

Out of Scope:

- Host hardening beyond Windows firewall changes
- Active attacker mitigation
- Multi-VM SIEM pipeline architecture

Lab Implementation Phases

Phase 1: Environment Setup

- Created a new Azure subscription and logged into portal
- Created resource group RG_SOC_Lab
- Deployed virtual network and subnet to support VM

Phase 2: Honeypot Deployment

- Created Windows 10 Pro VM named FIN-SQL-02
- Quota limitations required manual region and core adjustments
- Configured NSG to allow *all* inbound traffic (lab purposes only)
- Disabled Windows Firewall and confirmed VM received ICMP

Phase 3: Simulated Attack Traffic

- Connected via RDP and attempted several failed logins
- Monitored Windows Event Viewer for Event ID 4625
- Discovered real-world login attempts were already occurring

Phase 4: Sentinel Integration

- Created Log Analytics Workspace (LAW-Soc-Lab-001)
- Deployed Microsoft Sentinel and attached to workspace
- Installed Azure Monitor Agent on VM
- Created Data Collection Rule for forwarding security events

Phase 5: Log Enrichment with GeoIP

- Uploaded geoip-summarized.csv as a watchlist in Sentinel
- Used KQL's ipv4_lookup() function to correlate IP addresses with city, country, and geolocation fields
- Queried top 10 IPs by failed login count

KQL Example:

```
let GeoIPDB_FULL = _GetWatchlist("geoip");
SecurityEvent
| where EventID == 4625
| summarize FailedLoginCount = count() by IpAddress
| top 10 by FailedLoginCount desc
| evaluate ipv4_lookup(GeoIPDB_FULL, IpAddress, network)
| project IpAddress, cityname, countryname, latitude, longitude, FailedLoginCount
```

Phase 6: Visualization with Workbook

- Created a custom Sentinel Workbook
- Added map visualization with JSON-based heatmap
- Confirmed IP events plotted accurately across global regions

Screenshot:

Phase 7: Username Brute Force Analysis

- Queried the 20 most commonly attacked usernames
- Results included: admin, administrator, test, guest, etc.

KQL:

```
SecurityEvent

| where EventID == 4625

| summarize FailedLoginCount = count() by TargetUserName

| top 20 by FailedLoginCount desc
```

Outcome & Deliverables

- Deployed and tested fully functioning Azure honeypot
- Integrated with Sentinel for SIEM functionality
- Enriched logs with geographic context
- Visualized brute-force attempts in an interactive heatmap
- Demonstrated real-world attack data capture and KQL analysis

---

Contact

Joseph Hardy
Cybersecurity Graduate | Aspiring IT Security Professional
GitHub: JoHaa-D
Email: joseph.hardy603@gmail.com