

Deploying a SIEM in Microsoft Azure

Mentor: Dr. Masoud Sadjadi, Florida International University

Instructor: Dr. Masoud Sadjadi, Florida International University

Problem

Traditional security monitoring can often be reactive, relying on logs from real production systems that may miss attacks. It is difficult to get cleaned, targeted data on attacker **tactics, techniques, and procedures (TTPs)** without risking real assets.

This project addresses this gap by intentionally creating a vulnerable environment to capture and analyze this **critical attack data**, providing the successful information needed for a clear, **dynamic live attack map** visualization.

System Design

System Information and Event Management (SIEMs) are an extremely important aspect of large-scale cybersecurity.

SIEMs are able to:

- Collect logs from infrastructure.
- Identify threats.
- Gauge a system's overall defense.
- Make quick changes.

Current System

This project deploys a vulnerable honeypot in Azure to actively lure attackers and collect high fidelity threat intelligence logs in Microsoft Sentinel. By using **Kusto Query Language (KQL)** and **GeoIP mapping**, the system automates the analysis and visualization of attacker locations and intent, enhancing threat defense capabilities.

Object Design

When hosting a cloud server on **Azure**, it's important to maintain a high-level view of the environment to ensure it remains secure. Our project enables monitoring based on predefined rulesets. These rulesets **trigger alerts** when specific conditions are met, allowing for a quick action against threats to the environment.

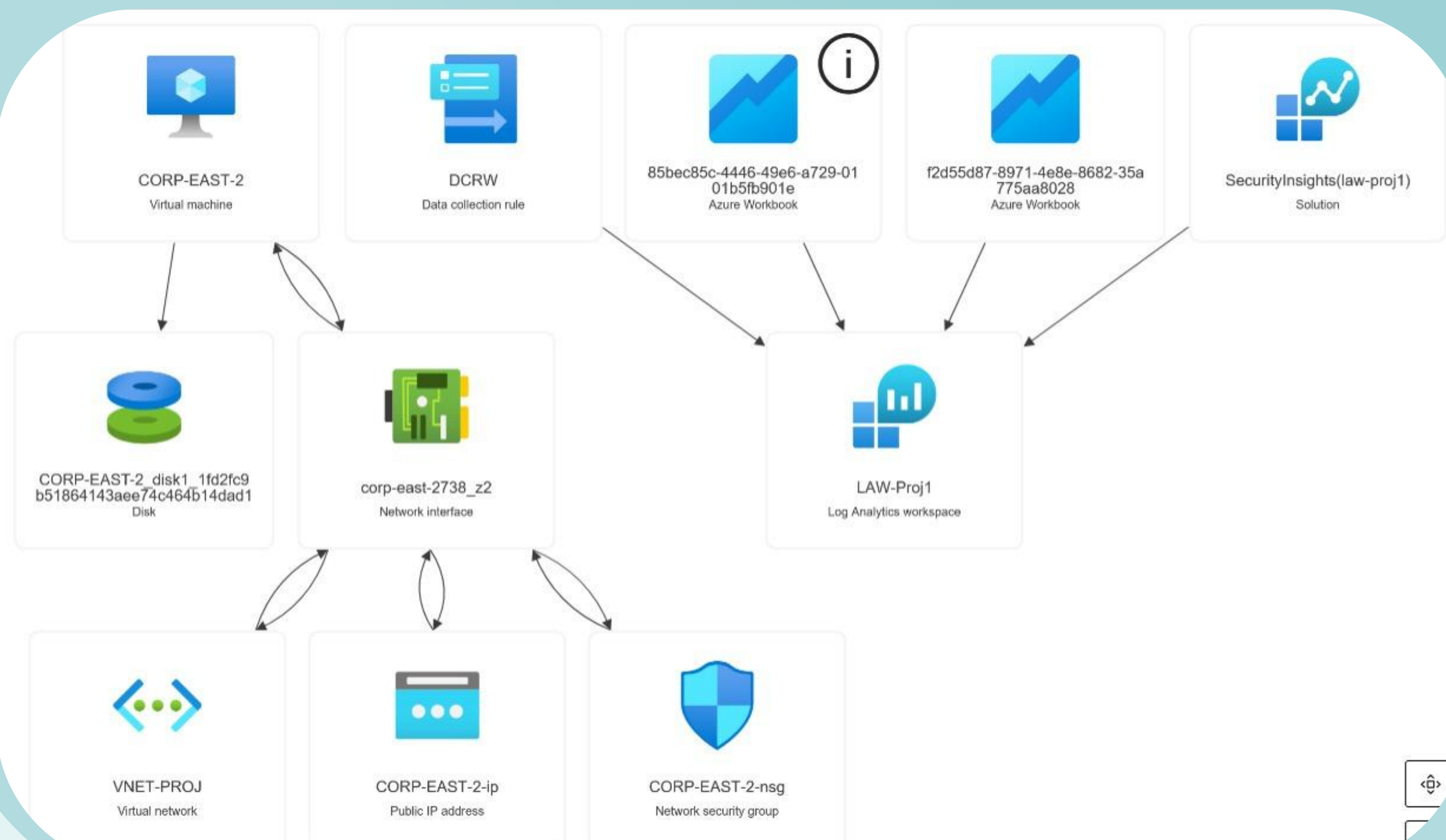
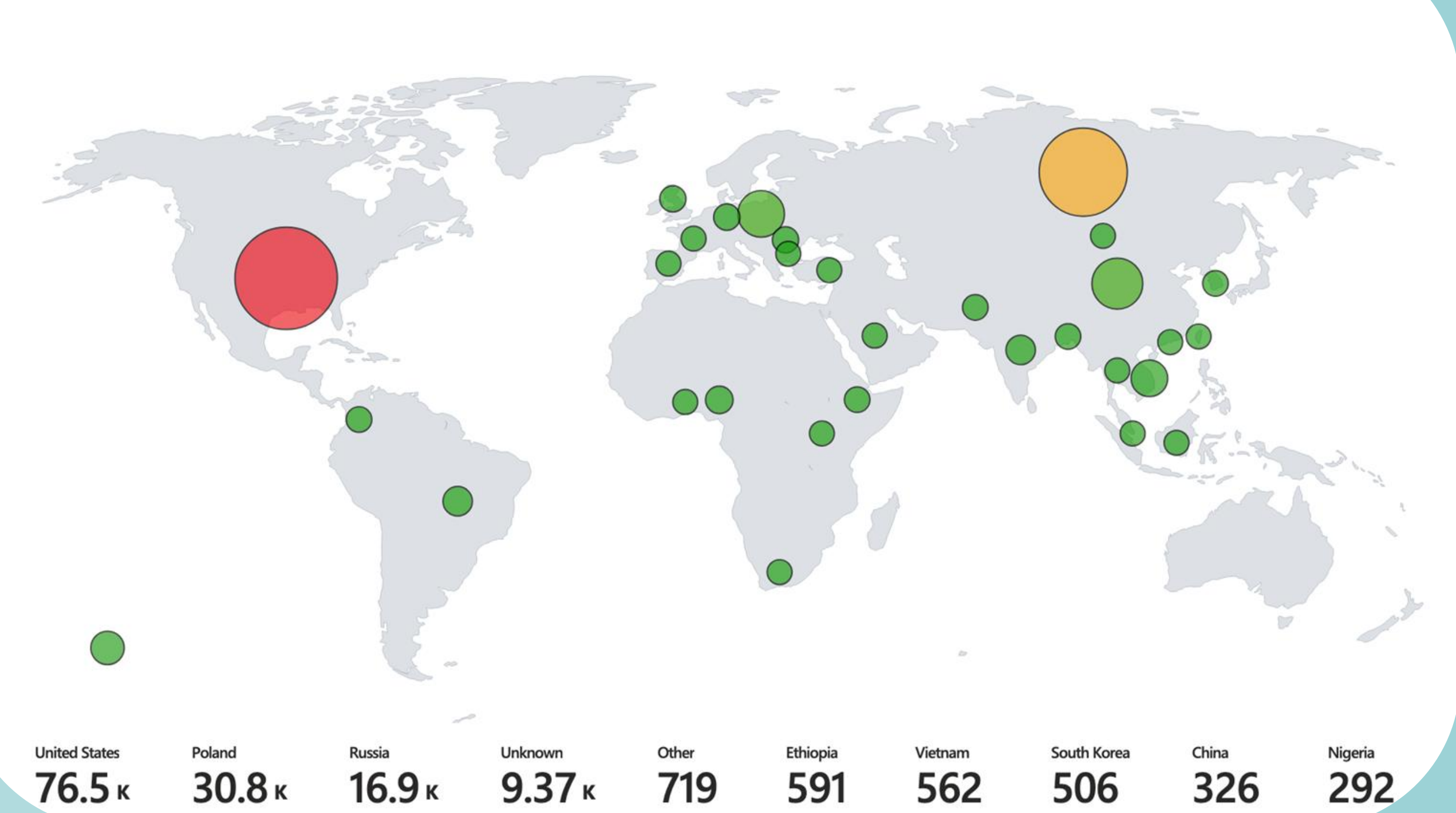
Requirements

Built out a SIEM in Azure using Microsoft Sentinel (integrated with **Azure Log Analytics Workspaces** and **Resource Groups** for organized log collection and analysis. Network activity was simulated by deploying a **Windows 10 honeypot** on a virtual network to capture malicious traffic. We aggregated failed login attempts recorded by the **Windows Event Viewer** and used **KQL** to filter relevant data. This filtered data was then used in Azure Workbooks to successfully build the dynamic, live attack map.

Implementation

We used **Virtual Machines (VMs)** in Azure to simulate various networked environments and capture attacks. Core Azure assets, including Log Analytics and integrated connectors, were used to **ingest and correlate statistics** from multiple resources. To validate the effectiveness of the SIEM, we created an attack map to show critical information like **attack volume** and **real-time location data**.

Global Map



Summary

Microsoft Sentinel provided practical insight into how cloud-native SIEMs enable real-time visibility and response in a **vulnerable network environment**.

The project emphasized **scalable log collection, rule-based filtering, and threat detection** through simulated attacks on Azure VMs. We built an attack map to provide a visual representation of our simulated system's security posture. Moving forward, integrating automation and expanding detection logic will generate **new, advanced telemetry** and further **strengthen the security posture**.

Acknowledgement

We thank **FIU** for assistance, cooperation and mentorship that we received throughout this process